CRIMINAL GROUP DATABASE: IMPACT AND USE POLICY

UPDATED: FEBRUARY 4, 2026

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that the criminal group database does not use artificial intelligence and machine learning.	Public comments highlighted a lack of industry-standard definitions for artificial intelligence or machine learning.
Expanded upon the criminal group database capabilities.	Added language clarifying the criminal group database capabilities. Added language describing how the criminal group database compliment other NYPD technologies.
Expanded upon the criminal group database rules of use.	Added language clarifying the criminal group database rules of use.
Expanded upon the criminal group database safeguard and security measures.	Added language regarding information security. Added language to reflect the removal of access to the criminal group database when job duties no longer require access.
Expanded upon the criminal group database data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon the criminal group database external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Grammar changes.	Minor syntax edits were made.

CRIMINAL GROUP DATABASE ADDENDUM

Date of Addendum	Addendum Description
October 13, 2023	Revised information regarding nomination criteria, nominating commands, nomination review, and removal review to reflect current NYPD policy.

CRIMINAL GROUP DATABASE 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

Information and intelligence gathering is a critical component of modern policing and an invaluable tool for detectives investigating crime. In support of its mission of reducing violent crime and protecting the public, the New York City Police Department's (NYPD) Criminal Group Database provides investigators with information about alleged gang members and additional intelligence relating to street gangs.

The NYPD produced this impact and use policy because the criminal group database is capable of sharing audio data, and both still and video images with NYPD investigators.

CAPABILITIES OF THE TECHNOLOGY

Often referred to as the "Gang Database," the NYPD Criminal Group Database, developed by SoundThinking, Inc. is used as an investigative resource to maintain consistent, up-to-date intelligence regarding criminal groups and street gangs. Based in an NYPD case management system,[1] the Criminal Group Database efficiently centralizes vital criminal group related intelligence that would otherwise be kept throughout different isolated data compartments within the NYPD.

Information such as criminal group names, associated incidents, geographic data, inter-criminal group dynamics and relationships, and alleged criminal group membership, including lawfully-obtained photographs, aliases, addresses, and known associations, is consolidated in such a way that NYPD investigators are able to discern trends, relationships, and patterns to enhance public safety, criminal investigations, and resource allocation.

Subjects cannot be entered into the NYPD Criminal Group Database automatically; inclusion data must be manually input into the database. If a person is fingerprinted by law enforcement, inclusion in the database does not appear in a person's criminal history or record of arrest. The NYPD Criminal Group Database cannot be accessed through the NYPD Domain Awareness System (DAS).[2] However, if DAS is used to search for information connected to a person included in the criminal group database, that inclusion will appear along with the name of the criminal group.

The Criminal Group Database does not use any biometric measuring technologies like facial recognition, and cannot conduct facial recognition analysis. [3]

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD's Criminal Group Database 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

Entry into the database is not proof of criminal behavior, it is simply an investigative lead. Entry alone is not grounds for a stop, arrest, or any other enforcement action. The database can only be

[1] For additional information on case management systems, please refer to the case management system impact and use policy.
[2] For additional information on DAS, please refer to the DAS impact and use policy.
[3] However, still images within the database 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.

accessed by limited authorized NYPD personnel. NYPD personnel may only access the database for legitimate law enforcement purposes or official business of the Department.

Activation: A subject may be included in the Criminal Group Database if one of two criteria are met. The first criteria requires the subject to exhibit some form of personal acknowledgement of criminal group membership, by either a self-admission of criminal group membership to a member of the NYPD or a self-admission of criminal group membership via the subject's own social media account(s).

A subject would be eligible for inclusion in the Criminal Group Database under the second criteria if, during the course of an investigation, there is a reasonable belief that the subject is a member of a criminal group, and that person is identified as a member of a criminal group by 2 independent and reliable sources, not including the nominating officer. Such reasonable beliefs must be supported by substantive explanations that the individual is a member of a criminal group.

A subject must be recommended for entry prior to the subject being included in the Criminal Group Database. NYPD personnel with authority to recommend a subject for entry into the database are limited to the following: Intelligence Bureau, Detective Bureau Borough Narcotics Commands, and Detective Bureau Gun Violence Suppression Units and its sub-commands.

A written narrative and supporting documentation must accompany the recommendation for Criminal Group Database entry. A supervisor of the qualified member of service submitting a candidate for nomination into the Criminal Group Database then reviews the materials and adopts the recommendation. The recommendation is then reviewed by the Real Time Crime Center, Social Media Analysis and Research Team and the Real Time Crime Center, Social Media Analysis and Research Team supervisor, who will either approve or reject the recommendation, or request additional analysis be performed before making a decision. If the Real Time Crime Center, Social Media Analysis and Research Team and Real Time Crime Center, Social Media Analysis and Research Team supervisor approves the recommendation, then the subject is entered into the database.

If a subject entered into the Criminal Group Database is under the age of 18, the nominating officer must notify a parent or guardian legally responsible for a subject that the subject has been included in the Criminal Group Database within 60 days of activation, unless the notification would interfere with active criminal investigations, and document the notification. The NYPD will conduct quarterly audits to ensure that notifications to parents of minors added to the Criminal Group Database are being made and documented.

Renewal & Deactivation: Subjects included in the Criminal Group Database must be reviewed to determine if their actions and records warrant continued inclusion. If a subject under the age of 18, the subject is reviewed every 2 years from date of entry. If the subject is 18 years old or older, the subject is reviewed every 3 years from date of entry. NYPD personnel are automatically notified when a subject is eligible for removal review. Subjects must be removed from the Criminal Group Database unless one of the following is true:

1. The subject was arrested for a violent crime, possession of a weapon, or any other crime committed in furtherance of the criminal group's activities, so long as the arrest is not sealed.

    - *Any such sealed arrest cannot be the basis for including or maintaining a subject in the Criminal Group Database. The NYPD will review subjects renewed based on an arrest every 6 months to ensure that the renewals are not based on arrests that were subsequently sealed;*

2. The subject is on parole or probation at the time of removal review; or
3. The Subject is in custody of any local city, state, or federal correctional facility or similar complex at the time of removal review.

Once a subject is removed from the database, the fact that they once were affiliated with a criminal group is permanently hidden from the database and NYPD computer systems.

Court Authorization: Court authorization is not required to use the Criminal Group Database. The Criminal Group Database only contains lawfully obtained information previously collected by NYPD personnel.

Additional Guidelines: If an NYPD investigation involving political activity requires the use of the criminal group database, 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 the Criminal Group Database 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 the Criminal Group Database.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Data Safeguard & Security Measures: The Criminal Group Database is confidential-password-protected and access is restricted to only authorized users who are authenticated by username and password. Access to the database is limited to personnel who have an articulable need for access in furtherance of lawful duty relating to the official business of the NYPD. Authorization must be requested by a Commanding Officer, and approved by the Detective Bureau (ITB). Access to the Criminal Group Database is determined by an officer's assignment and is rescinded once that officer's assignment no longer requires its use.

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

The Criminal Group Database 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. Authorized users are authenticated by username and password.

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 the classification of a case investigation record. The classification of case investigation records 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 it results in prosecution and appeals are exhausted, it results in a settlement, it results in no arrest, or when restitution is no longer sought.

The misuse of any 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 related to the NYPD Criminal Group Database 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 and NYPD policy.

EXTERNAL ENTITIES

Entities outside of the NYPD do not have direct access to the information and data collected by the NYPD's use of the Criminal Group Database.

If relevant to a criminal case, information is turned over 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 Criminal Group Database from the NYPD in accordance with applicable laws, regulations, and New York City and NYPD policies. The NYPD may provide information contained with the database to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, or disciplinary proceedings. Information is not shared in furtherance of immigration enforcement. Affirmation that a subject is included in the NYPD's Criminal Group Database may be shared with other law enforcement agencies in the course of conducting joint gang/criminal group investigations.

Information from the Criminal Group Database is not shared with the New York City Housing Authority or employers conducting background checks. Further, consistent with local law and NYPD policy, the Department does not share information in the database with Immigration and Customs Enforcement to conduct immigration enforcement, initiate deportation proceedings, or affect visa applications or citizen applications.

Following the laws of the State and City of New York, as well as NYPD policy, information contained in the database 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 Criminal Group Database 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 Criminal Group Database 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 the database 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 using the NYPD Criminal Group Database receive command-level training on the proper operation of the technology and associated equipment. NYPD personnel must operate the database in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Recommendation of a subject into the Criminal Group Database requires a written narrative and supporting documentation that justify inclusion of the subject in the database. Recommendations are reviewed by the supervisor of the qualified member of the service making the recommendation, the Real Time Crime Center, Social Media Analysis and Research Team, and the Real Time Crime Center, Social Media Analysis and Research Team supervisor who will either approve or reject the recommendation, or request additional analysis.

Subjects included in the Criminal Group Database must be reviewed to determine if their actions and records warrant continued inclusion. Activation and renewal reports contain a required field indicating the subject's next renewal date based on their age at the time the report is created. If a subject is under the age of 18, the subject is reviewed every 2 years from data of entry. If the subject is eighteen (18) years old or older, the subject is reviewed every 3 years from date of entry. NYPD personnel are automatically notified when a subject is eligible for removal review. Additionally, the NYPD has a mechanism for self-initiated review at any time. Once a subject is removed from the database, the fact that they once were affiliated with a criminal group is permanently hidden from the database

Supervisors of personnel who have access to the Criminal Group Database 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.

Immutable audit logs are created when any information is searched or accessed through the NYPD Criminal Group Database. 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 computer systems and equipment 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 the Criminal Group Database. 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 the Criminal Group Database.

DISPARATE IMPACTS OF THE TECHNOLOGY & IMPACT & USE POLICY

The NYPD has implemented significant safeguards to ensure that the Criminal Group Database is 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 the NYPD Criminal Group Database mitigate the risk of partial and biased law enforcement. The Criminal Group Database is an investigative resource to maintain consistent, up-to-date intelligence regarding criminal groups and street gangs. The Criminal Group Database efficiently centralizes vital criminal group related intelligence that would otherwise be kept throughout different isolated data compartments within the NYPD. The Criminal Group Database does not use any biometric measuring technologies.

Critics have asserted that inclusion in the Criminal Group Database disparately impacts people of color and has significant collateral consequences. Entry into the Criminal Group Database is not proof of criminal behavior, it is only an investigative lead. Entry alone is not grounds for a stop, arrest, or any other enforcement action. Moreover, New York State does not permit civil gang injunctions such as those routinely utilized in other jurisdictions. Unlike many states, New York does not have a sentencing enhancement for gang/criminal group members, nor a statute that criminalizes gang/criminal group membership. A subject's presence in the NYPD Criminal Group Database simply does not have the collateral consequences comparable to other jurisdictions. Based on these safeguards, any theoretical risks of the Criminal Group Database 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.