DATA ANALYSIS TOOLS:
IMPACT AND USE POLICY

UPDATED: FEBRUARY 4, 2026

SUMMARY OF CHANGES BETWEEN DRAFT AND FINAL POLICY

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

DATA ANALYSIS TOOLS 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

Daily operations of the New York City Police Department (NYPD) generate significant quantities of structured and unstructured data. Data analysis tools allow the NYPD to organize data within and across structured and unstructured datasets and allow for connections to be made faster and more efficiently than is possible by human effort alone.

The NYPD produced this impact and use policy because data analysis tools are capable of processing and sharing audio, video, location, and similar information contained within NYPD datasets.

CAPABILITIES OF THE TECHNOLOGY

In the course of its daily operations, the NYPD generates significant quantities of datasets, both structured and unstructured. Datasets are collections of information that can be read and processed by a computer. Structured data refers to data organized and contained in a fixed field or system (e.g., first/last name provided by a victim that is entered into fixed fields in an electronic records management system). Unstructured data refers to data that is not structured in a fixed manner (e.g., an audio file of a 911 call).

Data analysis tools are capable of performing search activity within and across datasets. In viewing the results, NYPD personnel may identify connections existing among otherwise isolated data compartments. For example, NYPD personnel can visualize assault complaints under investigation within a particular geographic area and identify potential links between investigations using data analysis tools.

Data analysis tools used by the NYPD include tools manufactured by Domino Data Labs and IBM Cognos Analytics. Additional tools have been withheld because disclosure would interfere with active investigations, and such information is not already publicly known. Disclosure would allow individuals to circumvent or manipulate the system to undermine its effectiveness. The redaction is narrowly tailored to prevent harm, while still providing meaningful transparency regarding the nature of the technology.

These tools do not use any biometric measurement technologies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD data analysis tools 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.

Data analysis tools are used by NYPD personnel to search structured and unstructured data generated by the daily operations of the NYPD. NYPD data analysis tools may only be used by NYPD personnel for legitimate law enforcement purposes.

Court Authorization: Court authorization is not required to use data analysis tools. NYPD data analysis tools process data that is lawfully generated by the NYPD or that has otherwise been

lawfully obtained, including through compliance with a court order, subpoena, or search warrant, stored in NYPD computer and case management systems.

Data analysis tools may be used in any situation the supervisory personnel responsible for oversight deems appropriate. The underlying facts, including the legitimate law enforcement purpose, are considered on a case-by-case basis prior to the utilization of the technology.

Additional Guidelines: If an NYPD investigation involving political activity requires the use of the data analysis tools, 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 data analysis tools 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 data analysis tools.

SAFEGUARD & SECURITY MEASURES AGAINST AUTHORIZED ACCESS

Access to data analysis tools is limited to authorized users who are authenticated by username and password. Authorization to use data analysis tools is only granted to NYPD personnel who have an articulable need to use the tools in furtherance of their job assignment. NYPD personnel access to data analysis tools is determined by the member of service's assignment and is rescinded when that assignment no longer requires its use.

Information located by use of data analysis tools is retained within an NYPD computer or case management system. Only authorized users have access to such information. 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. Authorized personnel must be authenticated by a username and password before records from the server may be accessed.

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 title 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 are 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 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

Information located by use of NYPD data analysis tools may only be used for legitimate law enforcement purposes or other official business of the NYPD including interference of criminal investigations, civil litigation, and disciplinary proceedings. Relevant information is stored in 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 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 will subject employees to administrative and potentially criminal penalties.

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

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

EXTERNAL ENTITIES

Entities outside of the NYPD do not have direct access to the information and data collected by the NYPD through its use of data analysis tools.

If the use of data analysis tools yields information related to a criminal case, the NYPD will turn it 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 computer or case management systems in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide information to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, and disciplinary proceedings. Information will not be shared in furtherance of immigration enforcement.

Following the laws of the State and City of New York, as well as NYPD policy, information 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 data analysis tools 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 data analysis tools' 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 identifying information 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 data analysis tools receive command level training on the proper operation of the supporting technology and the associated equipment. NYPD personnel must use data analysis tools in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

The use of data analysis tools, including the reasons for use, must be discussed with a supervisor. Supervisors of personnel utilizing data analysis tools 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.

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).

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 data analysis tools. 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 data analysis tools or associated equipment.

DISPARATE IMPACTS OF THE TECHNOLOGY & IMPACT & USE POLICY

The NYPD has implemented significant safeguards to ensure that data analysis tools 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 NYPD data analysis tools mitigate the risk of partial and biased law enforcement. Data analysis tools are only capable of performing search activity within and across structured and unstructured data generated by the daily operations of the NYPD. Data analysis tools do not use any biometric measuring technologies. NYPD data analysis tools policy integrates human investigators in all phases. Information located by a data analysis program alone does not constitute probable cause to effect an arrest or obtain an arrest or search warrant. Based on these safeguards, any theoretical risks of data analysis tools 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.