UNMANNED AIRCRAFT SYSTEMS: IMPACT AND USE POLICY

UPDATED: FEBRUARY 4, 2026

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

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

UNMANNED AIRCRAFT SYSTEMS ADDENDUM

Date of Addendum	Description of Addendum
September 8, 2023	Section detailing the rules, processes and guidelines relating to NYPD use of Unmanned Aircraft Systems updated to reflect approved uses.

UNMANNED AIRCRAFT 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

Unmanned aircraft systems (UAS), commonly referred to as "drones," are used by the New York City Police Department (NYPD) to respond to select priority emergency incidents, conduct search and rescue missions, disaster response, documentation of traffic collision and crime scenes, crowd monitoring, and provide a bird's eye view in dangerous active shooter and hostage situations. UAS help NYPD personnel gather crucial information as situations unfold without putting officers, civilian bystanders, and other involved parties at risk.

The NYPD produced this impact and use policy because NYPD UAS are capable of collecting video, thermal and location information, and sharing that information with NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

NYPD UAS are aircrafts without a human pilot onboard. The devices are controlled remotely by an NYPD operator via a handheld controller on scene or controller software at fixed NYPD command centers. The NYPD uses a variety of UAS from various manufacturers that will be outlined below. The UAS vary in size and are weather-resistant, equipped with multi-zoom cameras and thermal imaging capabilities.

UAS generally serve as a non-invasive compliment to other law enforcement and security measures employed by the NYPD. At large-scale events, UAS provide an expansive aerial view of a large area and can inform personnel deployments regarding congestion at these sites at a fraction of the cost and resources of other equipment.

UAS assist NYPD personnel responding to select priority emergency incidents, conducting search and rescue operations; documenting collisions and crimes scenes; searching for evidence at large or inaccessible scenes and hazardous material incidents; monitoring of vehicular traffic and pedestrian congestion at large events; providing visual assistance at hostage/barricaded suspect situations and at rooftop security situations during shooting incidents.

NYPD's Drone Fleet Capabilities:

The Skydio X10 has a max speed of 45 miles per hour. It has 360° obstacle avoidance and streams video to NYPD-issued smartphones[1] and select command centers. The X10 uses both telephoto camera with zoom capabilities and a thermal camera.[2] The NYPD uses the following attachments: speaker, spotlight, multi-purpose dropper (primarily used to drop a floatation device "Restube" at NYC Beach Deployments), and parachute. The X10 is capable of 3D modeling and mapping (used primarily for crime scene reconstructions).

The Skydio X2 has a max speed of 31 miles per hour. It has 360° obstacle avoidance and uses both a color and thermal camera. The X2 is capable of 3D modeling and mapping (used primarily for crime scene reconstructions).

[1] For additional information about Personal Electronic Devices (PEDs), please see the PEDs impact and use policy.
[2] For additional information about thermogenic cameras, please see the thermogenic cameras impact and use policy.

The DJI Matrice 350/300/30T/3T[3] have a max speed of 46-51 miles per hour. They have 360° obstacle avoidance and stream video to NYPD-issued smartphones and select command centers. The M350 uses a camera with zoom capabilities, a thermal lens, and infrared laser rangefinder. The NYPD uses the following attachments: speaker, spotlight, and multi-purpose dropper (primarily used to drop a floatation device "Restube" at NYC Beach Deployments). The DJI models are capable of 3D modeling and mapping (used primarily for crime scene reconstructions).

The DJI Avata has a max speed of 60 miles per hour. The Avata is small and agile for flying in tight spaces and through small openings. Its primary use is indoor and tactical flying. It does not stream video and has to be operated using First Person View goggles. Operations involving First-Person View UAS, per FAA guidelines, require a designated visual observer unless there is an active COA waiving the requirement.

The Brinc Lemur has a max speed of 48 miles per hour. It is small and agile for flying in tight spaces and small openings. Its primary use is indoor and tactical flying. The Lemur uses both a visual and thermal camera. It streams video to NYPD-issued smartphones and select command centers. The Lemur is equipped with an integrated spotlight, and a two-way audio system, consisting of a loudspeaker and a microphone affixed to the device, for hostage and barricaded incident communications. The NYPD uses the following attachments: speaker, spotlight, a multi-purpose dropper, and glass-breaker attachment with the Lemur.

The Nightingale Security Blackbird has a max speed of 33 miles per hour. It uses both a color and thermal camera. It streams video to NYPD-issued smartphones and select command centers. The Autel Evo II Pro is used solely for calibration.

Autonomous features of the UAS include orbiting (a maneuver that circles a scene) to gain situational awareness and waypoint missions (ex. back and forth patrol along the beach looking for dangerous conditions). Additionally, UAS may use object recognition to track a person or a vehicle if the UAS is assisting in a vehicular or foot pursuit. These autonomous features are done under the supervision of the UAS pilot.

NYPD UAS do not use biometric measuring technologies beyond the processing of thermal data. NYPD UAS do not use facial recognition technologies and cannot conduct facial recognition analysis.[4]

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

The NYPD's UAS must be used in a manner that is consistent with the requirements and protection of the Constitution of the United States, the New York State Constitution, and applicable statutory authorities.

[3] DJI systems were previously acquired and owned by the NYPD; all future procurements will comply with any new and applicable regulatory requirements.
[4] However, a still image can be created from the recorded video images and may be used as a probe image for facial recognition analysis. For additional information on facial recognition, please refer to the facial recognition impact and use policy.

NYPD policy directs that UAS may be used for the following purposes: search and rescue operations, documentation of collisions and crimes scenes, evidence searches at large or inaccessible scenes, hazardous material incidents, monitoring vehicular traffic and pedestrian congestion at large scale events, visual assistance at hostage/barricaded suspect situations, rapid response surveys at shootings or other crimes in progress, public safety, emergency, and other situations with the approval of the Chief of Department or designee.

UAS cannot be used for routine foot patrol by officers, traffic enforcement, or immobilizing a vehicle or suspect.

In situations where deployment of NYPD UAS has not been foreseen or prescribed in policy, the highest uniformed member of the NYPD, the Chief of Department or their designee, will decide if deployment is appropriate.

"Drone As First Responder" (DFR) Program:[5] The NYPD implemented the DFR program to enhance the situational awareness of responding officers, promote officer safety, and more effectively deploy NYPD resources. UAS are deployed remotely to select priority public safety calls, including searches for missing people, alerts from the ShotSpotter gunshot detection system, incidents of robberies and grand larcenies, and other crimes in progress as needed. The rapid deployment of DFR UAS, based at station houses, supplements the NYPD's in-person patrol, response to 911 calls by supplying high-definition video that is accessible, in real time, on officers and supervisors' NYPD-issued smartphones and select NYPD command centers. Audio is only available if a UAS has a speaker attached and only used in limited, emergency, circumstances. Most NYPD UAS are not deployed with this attachment and only provide video feeds.

Court Authorization: When UAS are used to conduct aerial surveillance of areas exposed to public observation, court authorization is not required prior to their use. Absent exigent circumstances, a UAS will not be used in areas where there is a reasonable expectation of privacy without NYPD personnel first obtaining a search warrant that explicitly authorizes the use of a UAS. After a search warrant is issued, a UAS may be used for a pre-warrant execution safety survey. The warrant will be obtained with the assistance of the prosecutor with jurisdiction over the matter.

Additional Guidelines: If necessary, 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 UAS will subject employees to administrative and potentially criminal penalties.

---

[5] *Mayor Adams, Interim Police Commissioner Donlon Announce 'Drone as First Responder' Program to Reduce Response Times and Keep New Yorkers Safe - NYC Mayor's Office* https://www.nyc.gov/mayors-office/news/2024/11/mayor-adams-interim-police-commissioner-donlon-drone-first-responder-program-to

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 UAS.

SAFEGUARDS & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

NYPD UAS may only be used and operated by trained NYPD personnel with valid pilot certificates. Operation of UAS must follow the guidelines of Title 14 of the Code of Federal Regulations, Part 107, and/or the Certificate of Authorization (COA) issued to the Department by the Federal Aviation Administration (FAA), as well as all other applicable FAA regulations and federal, state, and local laws. All NYPD personnel that operate a UAS have obtained their remote pilot certificate from the FAA and have passed the FAA's "Aeronautical Knowledge Test." If use is to take place outside of the NYPD's COA, NYPD personnel are instructed to contact FAA and seek a Special Government Interest COA prior to deployment.

NYPD personnel can request the response and deployment of a UAS when such request is connected to a public safety incident or emergency (including uses by other units like Emergency Service Unit and Highway Unit).

During non-emergency situations, the decision of whether to deploy NYPD UAS must be made by an NYPD executive serving as a commanding officer or executive officer, assigned to TARU. NYPD TARU personnel will then assess whether such use comports with NYPD policy and evaluate weather conditions, airspace restrictions, and safety in determining the appropriateness of use. If there is disagreement concerning the permissible use of a NYPD UAS, conferral with the Chief of Department will occur.

When appropriate, NYPD personnel make notifications to the NYPD Aviation Unit and Operations Unit of the time, location, and flight path prior to use of UAS in order to avoid any airspace conflict with other aircraft operating in the area. Radio dispatch must also be notified to alert responding NYPD members of a NYPD UAS in the area.

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

Data Safeguards & Security Measures: NYPD UAS transmit drone video footage over a secure network to an authorized vendor cloud environment. Video data is shared via secure cloud-to-cloud connection with other authorized vendor environments either for storage or viewing by authorized NYPD personnel. All drone footage is encrypted while drones are in transit or at rests and can only be accessed and decrypted through authorized vendor software.

Recordings obtained from UAS are retained within a cloud-based storage management system. Recordings may be downloaded to an NYPD computer or case management system. Only authorized users have access to these recordings. NYPD personnel utilizing computer and case

management systems are authenticated by username and password. Access to case management and computer systems is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty. Authorized users can only access data and perform tasks allocated to them by the system administrator according to their role.

The NYPD has a multifaceted approach to secure data and user accessibility within NYPD systems. The NYPD maintains an enterprise architecture (EA) program, which includes an architecture review process to determine system and security requirements on a case-by-case basis. System security is one of many pillars incorporated into the EA process. Additionally, all NYPD computer systems are managed by a user permission hierarchy based on rank and role via Active Directory (AD) authentication. Passwords are never stored locally; user authentication is stored within the AD. The AD is managed by a Lightweight Directory Access Protocol (LDAP) to restrict/allow port access. Accessing NYPD computer systems remotely requires dual factor authentication. All data within NYPD computer systems is encrypted both in transit and at rest via Secure Socket Layer (SSL)/Transport Layer Security (TLS) certifications which follow industry best practices.

NYPD personnel must abide by security terms and conditions associated with computer and case management systems of the NYPD, including those governing user passwords and logon procedures. NYPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the NYPD, only as required in the execution of lawful duty.

NYPD personnel are responsible for preventing third parties from unauthorized access to information. Failure to adhere to confidentiality policies may subject NYPD personnel to disciplinary and/or criminal action. NYPD personnel must confirm the identity and affiliation of individuals requesting information from the NYPD and determine that the release of information is lawful prior to disclosure.

Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

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

Videos obtained from UAS use will be retained for 39 months on the cloud-based platform. The NYPD's Legal Bureau may extend the retention period if the images are needed for civil litigation, subpoena production, Freedom of Information Law requests or other legal processes.

Recordings may only be used for legitimate law enforcement purposes or other official business of the NYPD, including in furtherance of criminal investigations, civil litigation, and disciplinary proceedings. Recordings will be stored in an appropriate NYPD computer or case management system. NYPD personnel utilizing case management and computer 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.

The NYPD retains and disposes of records pursuant to New York City Charter § 1133(f), (g) and (h). Pursuant to these provisions, the NYPD developed a retention schedule that was approved by the New York City Law Department and Department of Records and Information Services. This retention schedule governs the retention and disposition of NYPD records, and the NYPD retains and disposes of records pursuant to this schedule. The retention period of a "case investigation record" depends on its classification and is based on the final disposition of the case, i.e., what the arrestee is convicted of or pleads to. Further, case investigations are not considered closed unless they result in: prosecution and appeals are exhausted, a settlement, no arrest, or when restitution is no longer sought.

The misuse of any recording will subject employees to administrative and potentially criminal penalties.

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

Members of the public may request recordings obtained from the NYPD's use of UAS 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. Additionally, the NYPD voluntary discloses information related to UAS use on a quarterly basis on its website: (https://www1.nyc.gov/site/nypd/stats/reports-analysis/uas-drones.page).

EXTERNAL ENTITIES

Entities outside of the NYPD do not have direct access to the information and data collected by the use of NYPD UAS. However, entities outside of the NYPD may be given temporary access to NYPD UAS video feed, if requested.

If a UAS obtains data related to a criminal case, the NYPD will turn it over to the prosecutor with jurisdiction over the matter. The prosecutor will provide the data to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request information obtained by UAS from the NYPD. Such disclosure by the NYPD is governed by applicable laws and regulations, 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 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.

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;
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 UAS 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 UAS associated software or data in the performance of contractual duties to the NYPD. Such duties are typically technical or proprietary in nature (e.g., maintenance or failure mitigation). In providing vendors and contractors access to equipment and computer systems, the NYPD follows the principle of least privilege. Vendors and contractors are only allowed access on a "need to know basis" to fulfill contractual obligations and/or agreements.

Vendors and contractors providing equipment and services to the NYPD undergo vendor responsibility determination and integrity reviews. Vendors and contractors providing sensitive equipment and services to the NYPD also undergo background checks.

Vendors and contractors are legally obligated by contracts and/or agreements to maintain the confidentiality of NYPD data and information. Vendors and contractors are subject to criminal and civil penalties for unauthorized use or disclosure of NYPD data or information.

If recordings obtained using NYPD UAS 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 must obtain their FAA remote pilot certificate from the FAA and pass the FAA's "Aeronautical Knowledge Test" in order to operate a NYPD UAS. The exam covers the following topics: FAA regulations, airspace classifications and requirements, meteorology, emergency operations, aeronautical decision-making, flight inspections, airport operations, and others. Certification is valid for two years, and certificate holders must pass a recurrent knowledge test every two years.

Additionally, NYPD personnel assigned to operate a NYPD UAS must complete in-service training on UAS operations which encompasses further understanding of FAA regulations, as well as practice flights and simulations. NYPD personnel are required to demonstrate basic operational proficiency in accordance with standards established by the National Institute of Standards and Technology (NIST). NYPD personnel must operate UAS in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

NYPD personnel can request the response and deployment of a UAS when such request is connected to a public safety incident or emergency (including uses by other units like Emergency Service Unit and Highway Unit).

During non-emergency situations, the decision of whether to deploy NYPD UAS must be made by an NYPD executive serving as a commanding officer or executive officer, assigned to TARU. NYPD TARU personnel will then assess whether such use comports with NYPD policy and evaluate weather conditions, airspace restrictions, and safety in determining the appropriateness of use. If there is disagreement concerning the permissible use of a NYPD UAS, conferral with the Chief of Department will occur.

Every UAS mission conducted by the NYPD is documented on a "UAS Deployment Form." Flight log information is automated and entered directly on this form.

NYPD supervisors are responsible for the security and proper utilization of UAS equipment. 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 NYPD computer and case management systems are responsible for security and property 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.

Integrity Control Officers (ICOs) within each Command are responsible for maintaining the security and integrity of all information 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

General safety risks associated with UAS include personal injury and property damage resulting from loss of control of the aircraft due to pilot error, hardware malfunction, obstacle collision, or environmental factors. FAA guidelines specifically prohibit operation of UAS in a careless or reckless manner so as to endanger the life or property of another or allow an object to be dropped from the aircraft in a manner that creates an undue hazard. NYPD UAS manufacturers also include warnings against potential misuse and health-related disclosures of the UAS that could lead to serious injury or damage. Additionally, NYPS UAS use lithium-ion batteries, which present well-documented fire, explosion, and thermal runaway hazards. The FAA has documented a multitude of lithium battery related smoke, fire, and overheating incidents.

NYPD UAS are deployed by trained NYPD personnel under FAA and Department safety protocols. Some NYPD UAS are also equipped with parachutes as a precautionary measure and an added level of safety. When deployed in accordance with the criteria, limitations, and safeguards set forth in relevant law and policies, health and safety risks, potential operational issues, associated with UAS, are appropriately mitigated.

DISPARATE IMPACTS OF THE TECHNOLOGY & IMPACT & USE POLICY

The NYPD has implemented significant safeguards to ensure that UAS 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 UAS mitigate the risk of partial and biased law enforcement. NYPD supervisors are responsible for the security and proper utilization of UAS equipment. NYPD UAS do not contain facial recognition software and cannot conduct facial recognition analysis. Other than the processing of thermal data, NYPD UAS do not contain biometric measuring capabilities. Additionally, absent exigent circumstances, a UAS will not be deployed in areas where there is a reasonable expectation of privacy (e.g. to look inside of residences) without first obtaining a search warrant. Based on these safeguards, any theoretical risks of NYPD's UAS 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.