PORTABLE ELECTRONIC DEVICES: IMPACT AND USE POLICY

UPDATED: FEBRUARY 4, 2026

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

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

PORTABLE ELECTRONIC DEVICES ADDENDUM

Date of Addendum	Description of Addendum
April 11, 2023	NYPD smartphones issued to certain personnel assigned to the Criminal Justice, Detective, Patrol, Transit, and Housing Bureaus have access to a digital fingerprint scanning application on their device. A small number of NYPD smartphones have access to an augmented reality application for a pilot program.
December 7, 2023	Updated information related to utilization of biometric measurement technology to reflect use of digital fingerprint scanning application on portable electronic devices.

PORTABLE ELECTRONIC DEVICES 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

The New York City Police Department (NYPD) issues portable electronic devices (PEDs) to NYPD personnel to enable remote access to important information, enhance investigations, manage patrol, and communicate with members of the public.

The NYPD produced this impact and use policy because PEDs are capable of taking images of people, locations, license plates, and any other visual information, recording acoustic data, and providing location information to NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

The NYPD uses a variety of PEDs, such as smartphones, tablets, and laptops from a variety of manufacturers. Smartphones are distributed to all NYPD officers. Tablets are installed in many NYPD patrol vehicles. Select NYPD units and personnel are provided with laptops. NYPD personnel can use PEDs for a multitude of purposes, including but not limited to, preparing electronic reports about injured or sick people, vehicle accidents, and accessing their activity log. All NYPD-issued PEDs can connect to mobile and/or Wi-Fi networks, and can access location information through web mapping, navigation, and GPS applications.

Like nearly all modern smartphones, NYPD-issued smartphones contain a camera application that can be used to take photographs and record both still and video images. PEDs containing voice recording capabilities can be used to record acoustic data. PEDs contain a variety of useful applications, such as a translation application that aid officers when communicating with community members who do not speak English. They also contain a mobile version of the Domain Awareness System (DAS).[1] The mobile version of DAS allows NYPD personnel to remotely access NYPD databases, including real-time 911 data, Amber Alerts, and missing person alerts.

Augmented Reality: Additionally, NYPD-issued smartphones also contain an augmented reality application. This application is meant to provide officers in the field with easy-to-digest information regarding their surroundings, enhancing situational awareness and improving public safety. The application allows officers, through the use of their smartphone camera display, to augment their surroundings. Based on the officer's physical location, they are able to better visualize the pre-existing data contained within DAS in a more rapid and user-friendly manner. Data is not linked to individual's biometric information. The application does not have recording capabilities, nor does it employ facial recognition technology.[2]

NYPD-issued PEDs do not utilize any enhanced recording capabilities such as infrared, night vision, varying degrees of view, or long-ranged microphones. A small number of tablets have a peripheral device that allows for identification confirmation by a digital fingerprint scan, and certain NYPD personnel assigned to the Detective, Patrol, Transit, and Housing Bureaus have access to a mobile digital fingerprint scanning application on their NYPD-issued smartphones that allows for identification confirmation.[3]

[1] For additional information on DAS, please refer to the DAS impact and use policy.
[2] For additional information on the augmented reality application, please refer to the 2023 State of the NYPD address (beginning at 34:24): 2023 State of the NYPD - YouTube.
[3] For additional information on digital fingerprint scanning devices, please refer to the digital fingerprint scanning device impact and use policy.

NYPD personnel can use a fingerprint/facial identification feature to unlock some PEDs. NYPD-issued PEDs do not utilize any other kind of biometric measurement technologies. NYPD-issued PEDs cannot run facial recognition analysis.[4]

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD personnel must use all PEDs 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.

Access to NYPD PEDs is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. NYPD PEDs may only be used by NYPD personnel for legitimate law enforcement purposes or other official business of the NYPD. NYPD personnel are prohibited from using NYPD-issued PEDs to take photographs or record video of undercover officers, current or potential confidential informants, victims of a sex-crime, strip searches, and when present in a court or medical facility.

Court Authorization: A court order does not need to be obtained prior to using NYPD PEDs. NYPD PEDs are used in locations that do not enjoy a reasonable expectation of privacy, access the internet to view publicly available information, and provide remote access to lawfully obtained data and information previously obtained by the NYPD. Additionally, any information obtained from the augmented reality application must be separately verified.

Additional Guidelines: If necessary, the Intelligence Division will determine the need to use PEDs for NYPD investigations involving political activity. 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 PEDs 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 use of PEDs.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Data Safeguards & Security Measures: NYPD PEDs utilize an always on Virtual Private Network (VPN) to ensure the security of the data. The VPN ensures that all data goes through the NYPD network, allowing Active Directory to ensure only authorized members gain access to the data

[4] However, a still image created using a PED camera application 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.

requested. NYPD policy does not allow PEDs to connect to mobile hotspots. Access is determined by an officer's assignment and is rescinded when that officer's assignment no longer requires its use.

Data obtained by NYPD PEDs is retained within the appropriate NYPD computer or case management system. Only authorized users have access to the data. 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. 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

NYPD-issued PEDs store recorded data internally within the device itself. Internal storage capacity varies amongst NYPD-issued PEDs. Once the internal storage reaches its maximum capacity, the device cannot retain any new data. The NYPD-issued PED will not be able to record any new data until some of the memory is cleared. The augmented reality application uses pre-existing data from

NYPD databases and does not record, store, retain, or create any additional data.

Data obtained using NYPD-issued PEDs 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. Data relevant to an investigation are stored in an appropriate NYPD computer or case management system. The data may only be used for legitimate law enforcement purposes or other official business of the NYPD. 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 data 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 NYPD-issued PEDs 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

Entities outside of the NYPD do not have direct access to the information and data collected by NYPD-issued PEDs.

If an NYPD-issued PED captures data related to a criminal case, the NYPD will turn it over to the prosecutorial entity with jurisdiction over the matter in accordance with criminal discovery laws. Prosecutors will provide the data to the defendant(s) in accordance with the same criminal discovery laws.

Other law enforcement agencies may request data contained in NYPD PEDs or case management systems in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide data or information related to it to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, and disciplinary proceedings. Information is not shared in furtherance of immigration enforcement.

Following the laws of the State and City of New York, as well as NYPD policy, 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;
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 PEDs 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 PEDs 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 data obtained using NYPD-issued PEDs 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 officers utilizing NYPD-issued PEDs receive command-level training on the proper operation of the technology and associated equipment. Officers must operate PEDs in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

All NYPD personnel are advised that NYPD computer systems and equipment are intended for the purposes of conducting official business. 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. 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 PEDs activity from IAB, Commanding Officers, ICOs, Investigations Units, and others, may be made to the Information Technology Bureau.

HEALTH & SAFETY REPORTING

NYPD PEDs utilize lithium-ion battery packs. The NYPD adheres to standard manufacturer warnings for physical damage, charging hazards, and performance degradation. It is extremely unlikely that PEDs batteries would generate a fire under normal conditions of use.

DISPARATE IMPACTS OF THE TECHNOLOGY & IMPACT & USE POLICY

The NYPD has implemented significant safeguards to ensure that NYPD-issued PEDs are used effectively and responsibly. The NYPD does not believe that the technology has shown any potentially disparate impacts on 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-issued PEDs mitigate the risk of partial and biased law enforcement. Some tablets have a peripheral device that allows for identification confirmation by a digital fingerprint scan, and certain NYPD personnel assigned to the Detective, Patrol, Transit, and Housing Bureaus have access to a mobile digital fingerprint scanning application on their NYPD-issued smartphones that allows for identification confirmation. NYPD personnel can use a fingerprint/facial identification feature to unlock some PEDs. NYPD-issued PEDs do not utilize any other kind of biometric measurement technologies. Based on these safeguards, any theoretical risks of NYPD-issued PEDs 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.