



Effective Date: 05/25/2025	General Order Number: 9-09
Subject: FACIAL RECOGNITION TECHNOLOGY	
Amends / Supersedes: NEW	Review Required: ANNUALLY
VLEPSC Standards:	

FACIAL RECOGNITION TECHNOLOGY

A. PUPOSE

1. Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, and help in the identification of persons unable to identify themselves, or deceased persons. The Bristol Virginia Police Department has established access and use of a face recognition system to support the investigative efforts of law enforcement and public safety agencies.
2. It is the purpose of this policy to provide Bristol Virginia Police Department personnel with guidelines and principles for the collection, access, use, dissemination, retention, and purging of images and related information applicable to the implementation of a face recognition (FR) program. This policy will ensure that all FR uses are consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties (P/CRCL) of individuals.

Further, this policy will delineate the manner in which requests for face recognition are received, processed, catalogued, and responded to. The Fair Information Practice Principles (FIPPs) form the core of the privacy framework for this policy.

This policy assists the Bristol Virginia Police Department and its personnel in:

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of injury to specific individuals.

9-09: FACIAL RECOGNITION TECHNOLOGY

- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
 - Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
 - Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
 - Minimizing the threat and risk of damage to real or personal property.
 - Fostering trust in the government by strengthening transparency, oversight, and accountability.
 - Making the most effective use of public resources allocated to public safety entities.
3. All deployments of the face recognition system are for official use only/law enforcement sensitive (FOUO/LES). The provisions of this policy are provided to support the following authorized uses of face recognition information:
- To help identify an individual when there is a reasonable suspicion the individual has committed a crime.
 - To help identify a crime victim, including a victim of online sexual abuse material.
 - To help identify a person who may be a missing person or witness to criminal activity.
 - To help identify a victim of human trafficking or an individual involved in the trafficking of humans, weapons, drugs, or wildlife.
 - To help identify an online recruiter of criminal activity, including but not limited to human, weapon, drug, and wildlife trafficking.
 - To help a person who is suffering from a mental or physical disability impairing his ability to communicate and be understood.
 - To help identify a deceased person.
 - To help identify a person who is incapacitated or otherwise unable to identify himself.
 - To help identify a person who is reasonably believed to be a danger to himself or others.
 - To help identify an individual lawfully detained.

9-09: FACIAL RECOGNITION TECHNOLOGY

- To help mitigate an imminent threat to public safety, a significant threat to life, or a threat to national security, including acts of terrorism.
- To ensure officer safety as part of the vetting of undercover law enforcement.
- To determine whether an individual may have unlawfully obtained one or more state driver's licenses, financial instruments, or other official forms of identification using information that is fictitious or associated with a victim of identity theft.
- To help identify a person who an officer reasonably believes is concealing his true identity and about whom the officer has a reasonable suspicion has committed a crime other than concealing his identity.

Mobile face image searches may be performed only by an officer who has completed training meeting the requirements of subsections N.3 and N.5 and only during the course of an officer's lawful duties in furtherance of a valid law enforcement purpose listed within subsection A.3 of this policy, and excluding subsection F.5, in accordance with the conditions set forth in section F. (Refer to F. Use of Face Recognition Information).

B. POLICY APPLICABILITY AND LEGAL COMPLIANCE

1. This policy was established to ensure that all images are lawfully obtained, including face recognition probe images obtained or received, accessed, used, disseminated, retained, and purged by the Bristol Virginia Police Department. This policy also applies to:
 - Images contained in a known identity face image repository and its related identifying information.
 - The face image searching process.
 - Any results from face recognition searches that may be accessed, searched, used, evaluated, retained, disseminated, and purged by the Bristol Virginia Police Department.
 - Lawfully obtained probe images of unknown suspects that have been added to unsolved image files (refer to subsection L.3), pursuant to authorized criminal investigations.
2. All Bristol Virginia Police Department personnel requesting investigative support or relying upon facial recognition information, to include participating agency personnel, authorized individuals working in direct support of Bristol Virginia Police Department personnel, and other authorized users will comply with the Bristol Virginia Police Department's face recognition policy and will be required to complete the training referenced in subsection N.2.

9-09: FACIAL RECOGNITION TECHNOLOGY

In addition, authorized Bristol Virginia Police Department personnel tasked with processing face recognition requests and submissions, must also complete the specialized training referenced in subsection N.3.

An outside agency, or investigators from an outside agency, may request face recognition searches to assist with investigations only if all of the following criteria are met (unless there is a direct nexus to a Bristol Virginia Investigation see section G 1):

- Prior to making requests, the outside agency has a formalized agreement (e.g., a memorandum of understanding or an interagency agreement) between the Bristol Virginia Police Department and the outside agency and the agreement acknowledges that requesting investigators have an understanding of the training concepts listed in subsection N.4.
- The outside agency first provides examples of its applicable policies (e.g., privacy) and acknowledges in writing that its requesting investigators have an understanding of the training concepts listed in subsection N.4.
- The outside agency completes the Bristol Virginia Police Department's training identified in subsection N.4.
- The outside agency is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in subsection A.3 and the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number) and acknowledges an agreement with the following statement:

The result of a face recognition search is provided by the Bristol Virginia Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

3. The Bristol Virginia Police Department will provide a printed or electronic copy of this face recognition policy to all:
 - Bristol Virginia Police Department and non-Bristol Virginia Police Department personnel who provide services related to or in support of facial recognition.
 - Participating agencies
 - Individual authorized users
 - All requesting agencies and citizens of the Commonwealth

The Bristol Virginia Police Department will require both a written acknowledgment of receipt of this policy and a written agreement to comply with this policy and its applicable

9-09: FACIAL RECOGNITION TECHNOLOGY

provisions from all participating agencies and the Bristol Virginia Police Department's authorized users.

4. All Bristol Virginia Police Department personnel, participating agency personnel, and authorized individuals working in direct support of Bristol Virginia Police Department personnel (such as interns or volunteers), personnel providing information technology services to the Bristol Virginia Police Department, private contractors, agencies from which Bristol Virginia Police Department information originates, and other authorized users will comply with applicable laws and policies concerning P/CRCL, including, but not limited to, all applicable state or federal laws, regulations and policies that are, or reasonably should be known, and pertain to the use or operation of face recognition systems or federal P/CRCL laws.
5. The intent of the Bristol Virginia Police Department is that this policy will be scrupulously followed. It is recognized that law-enforcement can occur in a dynamic environment, with rapidly changing variables. Emergent/exigent deviations from this policy that do not otherwise violate the provisions of subsection A.3 are permissible with appropriate documentation to include the deviation, the justification for the deviation, and the approver, who must be the Chief of Police of the Bristol Virginia Police Department, The Deputy Chief or the Criminal Investigation Division Lieutenant. All deviations from this policy shall be made available to any person conducting an audit under subsection M.2. Exigent circumstances do not allow for deviations from § 15.2-1723.2(C), § 23.1-815.1(C), or § 52-4.5(D) of the Code of Virginia, or from subsection E.4, the use of trained examiners for the initial screening under subsection F.5, subsection F.6 and sections H, I, J, K, L, M, N (Excluding subsection N.4), and O.
6. Any facial recognition technology operator employed by the Bristol Virginia Police Department who (i) violates the agency's policy for the use of facial recognition technology or (ii) conducts a search for any reason other than an authorized use is guilty of a Class 3 misdemeanor and shall be required to complete training on the agency's policy on and authorized uses of facial recognition technology before being reinstated to operate such facial recognition technology (See § 15.2-1723.2(I), § 23.1-815.1(H), and § 52-4.5(G) of the Code of Virginia).

C. GOVERNANCE AND OVERSIGHT AUDIT

1. Primary responsibility for the operation of the Bristol Virginia Police Department's criminal justice information systems, face recognition program and system, operations, and the coordination of personnel; the receiving, seeking, retention, evaluation, data quality, use, purging, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Chief of Police of the Bristol Virginia Police Department.
2. The Bristol Virginia Police Department's Chief of Police will designate the Criminal Investigation Division Lieutenant to be responsible for the following (with the Deputy Chief/Major as backup/emergency designee):

9-09: FACIAL RECOGNITION TECHNOLOGY

- Overseeing and administering the face recognition program to ensure compliance with applicable laws, regulations, standards, and policy.
 - Acting as the authorizing official for individual access to face recognition information.
 - Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure “need-to-know” status.
 - Reviewing face recognition search requests, reviewing the results of face recognition searches and returning the most likely candidates—or candidate images—if any, to the requesting agency.
 - Ensuring that protocols are followed to ensure that face recognition information (including probe images) is automatically purged in accordance with the Bristol Virginia Police Department retention policy (refer to subsection L.1), unless determined to be of evidentiary value.
 - Ensuring user compliance with system requirements and the Bristol Virginia Police Department’s face recognition policy and applicable laws.
 - Confirming, through an audit conducted at least annually, that face recognition information is purged in accordance with this policy and to ensure compliance with applicable laws, regulations, standards, and policy.
 - Ensuring and documenting that personnel (including investigators from external agencies who may make face recognition search requests) meet all prerequisites stated in this policy prior to being authorized to use the face recognition system.
 - Publicly posting and reporting to the Virginia Department of Criminal Justice Services all required annual facial recognition technology use data (refer to section O. Agency Implementation and Reporting Requirements).
3. The Bristol Virginia Police Department’s face recognition program was established on June 1, 2025.
 4. The Bristol Virginia Police Department contracts with Lexis Nexis Risk Solutions to provide software and system development services for the entity’s face recognition system.
 5. The Bristol Virginia Police Department is guided by a committee made up of internal and external law enforcement staff that ensures that P/CRCL are not violated by this face recognition policy and by the Bristol Virginia Police Department face recognition information collection, receipt, access, use, dissemination, retention, and purging processes and procedures.

The committee will annually review and update the face recognition policy in response to changes in law and program implementation experience, including the results of audits and

9-09: FACIAL RECOGNITION TECHNOLOGY

inspections, and may solicit input from the Bristol Virginia Police Department's stakeholders on the development of the face recognition policy or proposed updates to the face recognition policy. The committee will ensure that this policy continues to conform to the Commonwealth's model facial recognition policy.

6. The Criminal Investigation Lieutenant will:
 - Receive reports regarding alleged errors and violations of the provisions of this face recognition policy or applicable state law.
 - Receive and coordinate complaint resolution under the Bristol Virginia Police Department's face recognition redress policy.
 - Ensure that the provisions of this policy and P/CRCL protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies.

The Criminal Investigation Division Lieutenant may be contacted at the following address: Bristol Virginia Police Department 551 Scott Street Bristol, Virginia 24201 (276) 645-7410 which is also posted on <https://www.bristolva.org/155/Police-Department>.

7. The Criminal Investigation Division Lieutenant will ensure that enforcement procedures and sanctions outlined in subsection M.3 are adequate and enforced.

D. DEFINITIONS

1. "Candidate Image" means an image within a rank-ordered list generated from a facial recognition search.
2. "Enhancement" means the process of adjusting digital images so that the results are more suitable for analysis or display (e.g., brightening, straightening, sharpening, etc.).
3. "Image Repository" means a securely managed collection of stored images and biometric templates attributable to specific individuals (i.e., any "pool" against which a probe image is compared).
4. "Facial recognition technology" means an electronic system or service for conducting an algorithmic comparison of images of a person's facial features for the purpose of identification. "Facial recognition technology" does not include the use of an automated or semi-automated process to redact a recording in order to protect the privacy of a subject depicted in the recording prior to release or disclosure of the recording outside of the law-enforcement agency if the process does not generate or result in the retention of any biometric data or surveillance information.
5. "Laptop Devices" means mobile devices with a full-featured operating system (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body.

9-09: FACIAL RECOGNITION TECHNOLOGY

This definition does not include pocket/handheld devices (e.g. smartphones), or mobile devices that feature a limited-feature operating system (e.g. tablets).

6. “Mobile Device” means any portable device used to obtain, access, use, or store facial recognition photos, data, or information via a wireless connection (e.g., cellular, Wi-Fi, Bluetooth, etc.).
7. “Pocket/Handheld Mobile Device” means devices (e.g. smartphones) intended to be carried in a pocket or holster attached to the body and feature an operating system with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.
8. “Probe Image” means a digital photograph suitable for use with facial recognition software for comparison to the known images contained within an image repository.
9. "Publicly Post" means to post on a website that is maintained by the entity or on any other website on which the entity generally posts information and that is available to the public or that clearly describes how the public may access such data.
10. “Tablet Device” means mobile devices with a limited-feature operating system (e.g. iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones) or mobile devices with full-featured operating systems (e.g. laptops).

E. ACQUIRING AND RECEIVING FACE RECOGNITION INFORMATION

1. The entity has authorized access to and can perform face recognition searches utilizing image repositories not owned by the entity.

By and through its contract with Lexis Nexis Risk Solutions the Bristol Virginia Police Department is authorized to access and perform face recognition searches utilizing the following external repositories:

- Facial recognition searches of public only facial imagery for the purposes of supporting official, authorized work of government agencies
2. For the purpose of performing face recognition searches, the Bristol Virginia Police Department and authorized Bristol Virginia Police Department personnel will obtain probe images or accept probe images from authorized requesting agencies or participating agencies only for the authorized uses identified in subsection B.2. Probe images should be a front-facing image of an individual and shall only be considered for use if lawfully obtained. Examples of probe images include but are not limited to:
 - Face images captured from closed circuit security cameras
 - Face images provided by a victim or witness to a crime

9-09: FACIAL RECOGNITION TECHNOLOGY

- Face images collected as evidence (fraudulent bank card or other photo ID).
3. The Bristol Virginia Police Department and, if applicable, any authorized requesting agencies or participating agencies, will not violate First, Fourth, and Fourteenth Amendments and will not perform or request face recognition searches about individuals or organizations based solely on their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, sexual orientations, or other classification protected by law.

However, the Bristol Virginia Police Department accords special consideration to the collection of face images relating to First Amendment-protected events, activities, and affiliations. Because of the sanctity of the First Amendment, law enforcement's role at First Amendment-protected events is usually limited to crowd control and public safety. Facial recognition technology shall not be intentionally used for the purpose of gathering intelligence related to First Amendment-protected speech, associations or activity. If, however, during the planning assessment and approval process for the particular event, before proceeding with the collection, the Bristol Virginia Police Department anticipates a need for the collection of face images, the Bristol Virginia Police Department will articulate whether collection of face images by law enforcement officers at the event is permissible; the legal or justified basis for such collection (including specifics regarding the criminal behavior that is suspected); and how face images may be collected, used, or retained, in accordance with this policy, as appropriate. If face images will be collected, the plan will specify the type of information collection that is permissible, identify who will collect face images (uniform or plainclothes officers), and define the permissible acts of collection.

The use of mobile face image capture devices relating to First Amendment-protected events, activities, and affiliations will be specially authorized by the Bristol Virginia Police Department in advance of the event.

The Bristol Virginia Police Department will reassess the need for and use of face recognition during the First Amendment-protected event. The Bristol Virginia Police Department will utilize face images from a First Amendment-protected event should the public safety mission change or in support of an active or ongoing criminal or homeland security investigation that occurs during or resulted from a First Amendment-protected event. If a criminal act is committed during the course of any such protected activity, the use of facial recognition technology shall be permitted for use solely to investigate the specific criminal actor(s) and identify victims or witnesses.

4. The Bristol Virginia Police Department will contract only with commercial face recognition companies or subcontractors that provide assurances that their methods for collecting, receiving, accessing, disseminating, retaining, and purging face recognition information comply with applicable local, state, tribal, territorial, and federal laws, as well as statutes, regulations, and policies and that these methods are not based on unfair or deceptive information collection practices.

9-09: FACIAL RECOGNITION TECHNOLOGY

F. USE OF FACE RECOGNITION INFORMATION

1. Access to or disclosure of face recognition search results will be provided only to individuals within the Bristol Virginia Police Department or in other governmental/law-enforcement agencies who are authorized to have access or have completed the applicable training outlined in section N, Training, and only for valid law enforcement purposes (e.g., enforcement, reactive investigations), and to IT personnel charged with the responsibility for system administration and maintenance. Authorized uses are described in subsection A.3 of this policy.
2. The Bristol Virginia Police Department prohibits access to and use of the face recognition system, including dissemination of face recognition search results, for the following purposes:
 - Non-law enforcement (including, but not limited to, personal purposes).
 - Any purpose that violates the U.S. Constitution or laws of the United States, including the protections of the First, Fourth, and Fourteenth Amendments.
 - Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by and secured by the U.S. Constitution or any other constitutionally protected right or attribute.
 - Harassing and/or intimidating any individual or group.
 - Using facial recognition technology for tracking the movements of an identified individual in a public space in real-time.
 - Enrolling a comparison image in a commercial image repository of a facial recognition technology service provider except pursuant to an authorized use.
 - Allow a facial recognition technology service provider to retain or further use a comparison image except as required for auditing that use or as may be otherwise required by law.
 - Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.
3. The Bristol Virginia Police Department shall not connect the face recognition system to any interface that performs live video surveillance, including surveillance cameras, drone footage, and body-worn cameras. The face recognition system will not be configured to conduct face recognition analysis on live video.
4. The Bristol Virginia Police Department will employ credentialed, role-based access criteria, as appropriate, to control:
 - Categories of face recognition information to which a particular group or class of users may have access, based on the group or class.

9-09: FACIAL RECOGNITION TECHNOLOGY

- The assignment of roles (e.g., administrator, manager, operator, and user).
 - The categories of face recognition information that a class of users are permitted to access, including information being utilized in specific investigations.
 - Any administrative or functional access required to maintain, control, administer, audit, or otherwise manage the information or equipment.
5. The following describes the Bristol Virginia Police Department's manual and automated face recognition search procedure, which is conducted in accordance with a valid law enforcement purpose and this policy.
- Authorized Bristol Virginia Police Department employees will submit a probe image of a subject of interest.
 - Only images of the actual person being sought in an investigation may be used for comparison via facial recognition technology. Images of other identified persons who reportedly resemble the description of a subject are also expressly prohibited for comparison.
 - Sketches, manually created images, digital renderings produced via software or with the aid of artificial intelligence, including predicted face morphology reports based on genetic information, shall not be queried via facial recognition technology in an effort to identify any unknown person.
 - This section shall not apply to images of missing endangered persons who are not the subject of a criminal investigation, such as age-progressed renderings of kidnapped or missing children.
 - Trained Bristol Virginia Police Department authorized examiners will initially run probe images without filters, using a filtered search as a secondary search, if needed. In some cases, enhancements may be considered after running an image as is against the image repository. Though enhancements to the probe image are permissible, examiners will not base any conclusions on a comparison between an enhanced probe image and a potential candidate photo. Examiners shall evaluate search results by comparing the original unknown probe image with the potential candidate photo.
 - In the automated search, most likely candidates are returned to the requestor ranked in order based on the similarity or confidence level.
 - The resulting candidates, if any, are then manually compared with the probe images and examined by an authorized, trained examiner. Examiners shall conduct the comparison of images, biometric identifiers, and biometric information in accordance with their training.

9-09: FACIAL RECOGNITION TECHNOLOGY

- If no likely candidates are found, the requesting entity will be informed of the negative results. In the case of a negative result, the images examined by the examiner will not be provided to the requesting entity.
- When feasible, examiners should submit the search and subsequent examination results for a peer or a supervisor review of the probe and candidate images, to include most likely candidate images, for verification and approval prior to dissemination. The approving peer or supervisor must be a trained examiner.
- All entities receiving the results of a face recognition search must be cautioned that the resulting candidate images do not provide positive identification of any subject, are considered advisory in nature as an investigative lead only, and do not establish probable cause, without further investigation, to obtain an arrest warrant without further investigation.
- The following statement will accompany the released most likely candidate image(s) and any related records:

The Bristol Virginia Police Department is providing this information as a result of a search, utilizing face recognition software, of records maintained by the Bristol Virginia Police Department. This information is provided only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

6. The Bristol Virginia Police Department has established the following process for mobile face recognition searches:
 - Bristol Virginia Police Department personnel shall not use pocket/handheld mobile devices to conduct facial recognition analysis. This prohibition does not preclude the use of a pocket/handheld mobile device to transmit or capture a probe image.
 - Bristol Virginia Police Department personnel shall only use laptop or tablet devices of sufficient screen size and resolution so as to effectively complete a morphological comparison of a probe image with the most likely candidate image(s).
 - Only Bristol Virginia Police Department officers authorized and trained in accordance with subsections N.3 and N.5 may utilize mobile face recognition and only on Bristol Virginia Police Department -authorized devices. No personal mobile devices shall be permitted to use or access the Bristol Virginia Police Department facial recognition system.
 - Prior to utilizing a face recognition search, an officer should first attempt to ascertain an individual's identity by means other than a face recognition search, such as requesting identification, using a fingerprint scanner, etc.

9-09: FACIAL RECOGNITION TECHNOLOGY

- Mobile searches may be performed during the course of an officer's lawful duties and only for the entity-established authorized uses listed in section A. Purpose Statement, subsection 3.
- In addition, officers may only capture an individual's image when one of the conditions listed in subsection F.7 exist.
- The face recognition system does not work over standard cellular internet. Officers must log in and be authenticated into the Bristol Virginia Police Department law enforcement network in order to access the face recognition system.
- The log-in screen will prompt the user to acknowledge and agree to the following statement before granting access to the system:
 - Search results from Clearview AI should not be considered as conclusive intelligence or evidence admissible in Court. Search results from Clearview AI are for lead generation only and must be independently verified.
 - Clearview AI is to be used solely as authorized by a government agency. Use of Clearview AI for any other purpose is strictly prohibited.
 - Your entire search history on Clearview AI will be monitored and accessible to the appointed administrator within your organization. Customer search histories remain confidential and are not accessible to Clearview AI.
 - Do not share passwords or accounts. Use of Clearview AI products is strictly limited to devices that are owned, issued, or managed by the government. Personal devices must not be used for accessing Clearview AI products.
 - Do not use Clearview AI in a way that violates any local state or national law.
- Prior to executing the search, the officer must enter the reason for the search. A reason permitted under subsection A.3 shall be entered. If applicable, a condition under subsection F.7 shall also be entered.
- The captured image (probe image) will be submitted to the face recognition system, which will compare the probe image with those contained in the on the open web searched by Lexis Nexis – Clearview – AI.
- A list of most likely candidate images is returned ranked by computer-evaluated similarity.
- The officer then completes a visual or manual morphological comparison of the candidate images with the subject's probe image to make a visual judgment, as well as uses standard investigative techniques, to determine whether the subject is the same as a candidate image.

9-09: FACIAL RECOGNITION TECHNOLOGY

7. Authorized and trained Bristol Virginia Police Department officers may only capture a probe image for a facial recognition search during the course of lawful duties, in accordance with Bristol Virginia Police Department -established authorized uses (refer to section A. Purpose Statement, subsection 3), and when one of the following conditions exist:
 - Public Place: In accordance with applicable law, the individual's image is captured in a public place for the purpose of identification and the individual has no reasonable expectation of privacy. The Bristol Virginia Police Department will not authorize the collection of the individual's face image when the individual raises an objection that is recognized by law (e.g., religious objection).
 - Consent: The individual consents to have his or her image captured for the purpose of identification. The individual may withdraw consent at any time. If consent is withdrawn and neither of the other conditions applies, then use of a face recognition search is not authorized, and the search must stop immediately.
 - Incapacitation, Defect, or Death: When an individual is unable to provide reliable identification because of physical incapacitation or defect, mental incapacitation or defect, or death, and an immediate identification is needed to assist the officer in the performance of his or her lawful duties.
 - Lawful Detention: In cases where an individual's image has been captured while lawfully detained.

G. SHARING AND DISSEMINATING FACE RECOGNITION INFORMATION

1. **Unless there is a direct nexus to a criminal investigation/case in the City of Bristol, Virginia the Bristol Virginia Police department will not allow external law enforcement agencies to request facial recognition searches.** Any and all multi agency criminal investigative facial recognition search requests that have a direct nexus to a criminal case being handled by the Bristol Virginia Police Department will be processed by the Criminal Investigation Division Lieutenant or emergency designee. The Criminal Investigation Division Lieutenant (or emergency designee) will document the agencies involved in the investigation, their respective case number(s), and assigned personnel. The related Bristol Virginia case number, and assigned personnel will also be recorded.
2. The following statement will be provided to any and all agencies engaged in a joint investigation with the Bristol Virginia Police Department in which facial recognition is used:

The Bristol Virginia Police Department is providing this information as a result of a search, utilizing face recognition software, of records maintained by the Bristol Virginia Police Department. This information is provided only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

9-09: FACIAL RECOGNITION TECHNOLOGY

3. Agencies involved in a joint investigation with the Bristol Virginia Police Department will be notified that **face recognition search information is not to be:**
 - Sold, published, exchanged, or disclosed to commercial or private entities or individuals except as required by applicable law and to the extent authorized by the Bristol Virginia Police Department's agreement with the commercial vendor.
 - Disclosed or published without prior notice to the originating entity that such information is subject to disclosure or publication. However, the Bristol Virginia Police Department and the originating agency may agree in writing in advance that the Bristol Virginia Police Department will disclose face recognition search information as part of its normal operations, including disclosure to an external auditor of the face recognition search information.
 - Disclosed on a discretionary basis unless the originating agency has provided prior written approval or unless such disclosure is otherwise authorized by the MOU or agreement between the Bristol Virginia Police Department and the originating agency.
 - Disclosed to unauthorized individuals or for unauthorized purposes.
 - Disclosed by the Bristol Virginia Police Department's commercial face recognition vendor, if any, without the express written permission of the Bristol Virginia Police Department
4. The Bristol Virginia Police Department will not confirm the existence or nonexistence of face recognition information to any individual or agency that would not be authorized to receive the information unless otherwise required by law.

H. DATA QUALITY ASSURANCE

1. Original probe images will not be altered, changed, or modified in order to protect the integrity of the image. Any enhancements made to a probe image will be made on a copy, saved as a separate image, and documented to indicate what enhancements were made, including the date and time of change.
2. Bristol Virginia Police Department examiners will analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a face recognition search.
3. **The Bristol Virginia Police Department considers the results, if any, of a face recognition search to be advisory in nature as an investigative lead only.** Face recognition search results are not considered positive identification of a subject and do not, on their own, not establish probable cause and shall not be included in any affidavit. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

9-09: FACIAL RECOGNITION TECHNOLOGY

All potential matches are considered advisory in nature and any subsequent verification of the individual's identity, such as through a fingerprint check, or follow-on action should be based on an agency's standard operating procedures.

4. The Bristol Virginia Police Department will perform routine maintenance, upgrades and enhancements, testing, and refreshes of the face recognition system to ensure proper performance, including the following:
 - Designated, trained personnel shall assess the face recognition system on a regular basis to ensure performance and accuracy.
 - Malfunctions or deficiencies of the system will be reported to the Chief of Police within 24 hours of discovering the malfunctions or deficiencies.
5. The integrity of information depends on quality control and correction of recognized errors, which is key to mitigating the potential risk of misidentification or inclusion of individuals in a possible identification. The Bristol Virginia Police Department will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The Bristol Virginia Police Department will correct the information or advise the process for obtaining correction of the information.

I. DISCLOSURE REQUESTS

1. Face recognition information will be disclosed to the public in accordance with federal and state retention and public records laws. A record will be kept of all requests and of what information is disclosed to an individual.

J. REDRESS

J.1 COMPLAINTS

1. If an individual has a complaint with regard to face recognition information that is exempt from disclosure, is held by the Bristol Virginia Police Department and allegedly has resulted in demonstrable harm to the complainant, Bristol Virginia Police Department will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the Bristol Virginia Police Department Administration Captain at the following address: 551 Scott Street Bristol, Virginia 24201. The Administration Captain will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law.

If the face recognition information did not originate with the Bristol Virginia Police Department, the Administration Captain will notify the originating agency within 30 days in writing or electronically and, upon request, assist such agency to correct any

9-09: FACIAL RECOGNITION TECHNOLOGY

identified data/record deficiencies in the information or verify that the record is accurate.

All face recognition information held by the Bristol Virginia Police Department that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged or out-of-date information. If there is no resolution within 30 days, the entity will not share the information until such time as the complaint has been resolved. A record will be kept by the entity of all complaints and the resulting action taken in response to them.

All complaints filed under this subsection J.1 shall be made available to any person conducting an audit under subsection M.2.

J.2 REQUESTS FOR CORRECTIONS

1. If, in accordance with state law, an individual requests correction of face recognition information originating with the Bristol Virginia Police Department that has been disclosed, the Bristol Virginia Police Department's Criminal Investigation Division Lieutenant will inform the individual of the procedure for requesting a correction. The Bristol Virginia Police Department will investigate, in a timely manner, alleged errors and malfunctions or deficiencies of face recognition information or, if applicable, will request that the originating agency or vendor investigate the alleged errors and malfunctions or deficiencies. The Bristol Virginia Police Department will correct the information or advise the process for obtaining correction of the information. A record will be kept of all requests and the Bristol Virginia Police Department's response.

J.3 APPEALS

1. The individual who has requested disclosure or to whom face recognition information has been disclosed will be informed of the reason(s) why the Bristol Virginia Police Department or originating agency denied the request for disclosure or correction. The individual will also be informed of the procedure for appeal when the Bristol Virginia Police Department or originating agency has cited an exemption for the type of information requested or has declined to correct challenged face recognition information to the satisfaction of the individual to whom the information relates.

K. SECURITY AND MAINTENANCE

1. The Bristol Virginia Police Department will comply with generally accepted industry or other applicable standards for security, in accordance with Commonwealth of Virginia and FBI CJIS Security standards to protect data at rest, in transit, or in use. Security safeguards will cover any type of medium (printed or electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related Bristol Virginia Police Department activity.

The Bristol Virginia Police Department and Lexis Nexis Risk Solutions will operate in a secure environment protected from external intrusion and will utilize secure internal and

9-09: FACIAL RECOGNITION TECHNOLOGY

external security and privacy safeguards against network intrusions, such as strong multifactor authentication; encrypted communications; firewalls; and other reasonable physical technological, administrative, procedural, and personnel security measures to minimize the risks of unauthorized access to the system. Access to the Bristol Virginia Police Department's face recognition information from outside the facility will be allowed only over secure networks.

All results produced by the Bristol Virginia Police Department as a result of a face recognition search are disseminated by secured electronic means (such as an official government e-mail address). Non-electronic disseminations will be conducted personally or by phone with the requestor or designee.

2. All individuals with access to Bristol Virginia Police Department information or information systems will report a suspected or confirmed breach to the Bristol Virginia Police Department's Criminal Investigation Division Lieutenant as soon as possible and without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, and electronic.

Following assessment of the suspected or confirmed breach and as soon as practicable, the Bristol Virginia Police Department will notify the originating agency from which the Bristol Virginia Police Department received face recognition information of the nature and scope of a suspected or confirmed breach of such information.

The Bristol Virginia Police Department will adhere to the City of Bristol's policy governing data breach notification. In accordance with the City of Bristol Virginia Information Technology Privacy Management and Incident Response Plan 2023, the Bristol Virginia Police Department will provide effective and appropriate response procedures to events and situations that may expose personally identifiable information (PII) of both citizens and staff as well as legal records collected and maintained by the City of Bristol Virginia to unauthorized individuals, both internally and externally. The Bristol Virginia Police Department will determine whether a data breach requires notification to an affected individual, in accordance with applicable laws, regulations, policies, and procedures.

3. All face recognition equipment and face recognition software and components will be properly maintained in accordance with the manufacturer's recommendations, including routine updates as appropriate.
4. Lexis Nexis Risk Solutions will store face recognition information in a manner that ensures that it cannot be modified, accessed, or purged except by personnel authorized to take such actions.
5. Authorized access to the Bristol Virginia Police Department face recognition system will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and the training referenced in section N. Training.

9-09: FACIAL RECOGNITION TECHNOLOGY

6. Usernames and passwords to the face recognition system are not transferrable, must not be shared by Bristol Virginia Police Department personnel, and must be kept confidential.
7. The system administrator will ensure that all manufacturer-generated default passwords are replaced with secure passwords before web-based interfaces of the system become operational. User passwords must meet the following standards No English words and a combination of upper and lowercase letters, numbers, and at least two special characters. Authorized users are not permitted to use the same password over time and are required to change their password every sixty days.
8. Queries made to the Bristol Virginia Police Department's face recognition system will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit.
9. The Bristol Virginia Police Department will maintain an audit trail of requested, accessed, searched, or disseminated Bristol Virginia Police Department held face recognition information. An audit trail of requests, access, and searches of face recognition information for specific purposes, and information disseminated in response to the request shall be maintained in accordance with Records Retention and Disposition Schedules promulgated by the Library of Virginia.¹

Audit logs will include:

- The name, agency, and contact information of the law enforcement user
- The date and time of access
- Case number
- Probe images (refer to subsection L.5)
- The specific information accessed
- The modification or deletion, if any, of the face recognition information
- The authorized law enforcement or public safety justification for access that is consistent with section E (criminal investigation, criminal intelligence, imminent threat, or identification), including a relevant case number if available).

¹ For state agencies: GS-101, 100336 - Management Reports: Other Reports
For local agencies: GS-19; 010065: Management Reports
The recommended retention period for these records is three years.

9-09: FACIAL RECOGNITION TECHNOLOGY

L. INFORMATION RETENTION AND PURGING

1. Bristol Virginia Police Department has authorized access to and can perform face recognition searches utilizing image repositories not owned by the Bristol Virginia Police Department.

Images accessed by the Bristol Virginia Police Department for face recognition searches, in accordance with subsection E.1, are not maintained or owned by the Bristol Virginia Police Department and are subject to the retention policies of the respective agencies authorized to maintain those images.

Once a face recognition image is downloaded by Bristol Virginia Police Department personnel and incorporated into a criminal intelligence record or an investigative case file, the face recognition information is then considered criminal intelligence or investigative information and the laws, regulations, and policies applicable to that type of information or criminal intelligence govern its use.

Any images that do not originate with the Bristol Virginia Police Department will remain in the custody and control of the originating agency and will not otherwise be transferred to any other entity without authorization from the originating agency.

If the face recognition image has become or there is reason to believe that it will become evidence that tends to inculcate or exculpate a suspect, in a specific criminal or other law enforcement investigation or action, the following provisions apply:

- In those circumstances in which an image is identified as material having evidentiary value, the face recognition CID Lieutenant or designee will review the facts of the specific case and determine whether the image should be retained beyond the established retention period. If it is determined that it is reasonable to believe the image has evidentiary value, the face recognition CID Lieutenant will authorize the transfer of the applicable image from the image repository to the Bristol Virginia Police Department's investigative case file/records management system.

The Bristol Virginia Police Department retains the right to remove images from the repository earlier than the retention period, based on the limitations of information storage requirements and subject to any applicable record retention laws and statutory disclosure mandates. Early removal, however, will not be used as a means for intentionally interfering with a lawful complaint or a public records request. The retention period may be modified at any time by the Bristol Virginia Police Department, subject to applicable legal requirements.

2. Probe images are not enrolled (stored) in the image repository. Retention of probe images will be the same as for the type of file (criminal case file, criminal intelligence file), whether paper or electronic, in which the information is stored.

9-09: FACIAL RECOGNITION TECHNOLOGY

3. A lawfully obtained probe image of an unknown suspect may be added to an unsolved image file pursuant to an authorized criminal investigation. Images in an unsolved image file are periodically compared with those in an image repository (of known persons). If a most likely candidate meets a minimum threshold of computer-evaluated similarity results, the contributor of the probe image is notified and requested to validate the continued need to store the image or determine whether the image can be purged. Images enrolled in an unsolved image file will be validated on a periodic basis, at least every ninety (90) days, by the contributors to ensure that the criminal investigation remains active and that the image remains relevant to the investigation. If, in accordance with this policy, the contributor has not validated the need to retain the image in the unsolved file, the image will be purged.
4. The list of most likely candidate images is not enrolled (stored) in the image repository. For Bristol Virginia Police Department investigations, the case agent will maintain the list of most likely candidates from a face recognition search within the case file.
5. Probe images and face recognition search results are saved within the entity's system audit log, for audit purposes only. The audit log is available only to the Criminal Investigation Division Lieutenant and will be purged within two years. The audit log is not searchable and face recognition searches cannot be performed using the audit log.

M. ACCOUNTABILITY AND ENFORCEMENT

M.1 TRANSPARENCY

1. The Bristol Virginia Police Department will be open with the public with regard to face recognition information collection, receipt, access, use, dissemination, retention, and purging practices. The Bristol Virginia Police Department's face recognition policy will be made available in printed copy upon request and Publicly Posted on the Bristol Virginia Police Department website at <https://www.bristolva.org/155/Police-Department>.
2. The Bristol Virginia Police Department's Criminal Investigations Division Lieutenant will be responsible for receiving and responding to inquiries and complaints about the entity's use of the face recognition system, as well as complaints regarding incorrect information or P/CRCL protections in the image repository maintained and face recognition system accessed by the Bristol Virginia Police Department. The Criminal Investigations Division Lieutenant may be contacted at bvacop@bristolva.org.

M.2 ACCOUNTABILITY

1. The Bristol Virginia Police Department will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with the face recognition system requirements and with the provisions of this policy and applicable law. This will include logging access to face recognition information, may include any type of medium or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related activity, and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions.

9-09: FACIAL RECOGNITION TECHNOLOGY

These audits will be mandated at least semi-annually and a record of the audits will be maintained by the Criminal Investigations Division Lieutenant of the Bristol Virginia Police Department pursuant to the retention policy. Audits may be completed by an independent third party or a designated representative of the Bristol Virginia Police Department.

Appropriate elements of this audit process and key audit outcomes will be compiled into a report and may be provided to command staff and oversight entities or governance boards.

2. The Bristol Virginia Police Department's personnel or other authorized users shall report errors, malfunctions, or deficiencies of face recognition information and suspected or confirmed violations of the Bristol Virginia Police Department's face recognition policy to the Bristol Virginia Police Department.
3. The Criminal Investigations Lieutenant will review and update the provisions contained in this face recognition policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the face recognition system; the audit review; and public expectations.

M.3 ENFORCEMENT

1. If Bristol Virginia Police Department personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, receipt, access, use, dissemination, retention, and purging, the Chief of Police of the Bristol Virginia Police Department will:
 - Suspend or discontinue access to information by the Bristol Virginia Police Department entity personnel, the participating agency, or the authorized user.
 - Apply appropriate disciplinary or administrative actions or sanctions.
 - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

The Bristol Virginia Police Department reserves the right to establish the qualifications and number of personnel having access to the Bristol Virginia Police Department's face recognition system and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating this face recognition policy.

N. TRAINING

1. Before access to the Bristol Virginia Police Department's face recognition system is authorized, the Bristol Virginia Police Department will require the following individuals to participate in training regarding implementation of and adherence to this face recognition policy:

9-09: FACIAL RECOGNITION TECHNOLOGY

- All authorized Bristol Virginia Police Department personnel, including examiners
 - All authorized participating agency personnel
 - All authorized personnel providing information technology services to the Bristol Virginia Police Department
2. The Bristol Virginia Police Department face recognition policy training program will cover both:
- a. Elements of the operation of the face recognition program, including:
 - Purpose and provisions of the face recognition policy.
 - Substance and intent of the provisions of this face recognition policy and any revisions thereto relating to collection, receipt, access, use, dissemination, retention, and purging of the Bristol Virginia Police Department's face recognition information.
 - Policies and procedures that mitigate the risk of profiling.
 - How to implement the face recognition policy in the day-to-day work of the user, whether a paper or systems user.
 - Security awareness training.
 - How to identify, report, and respond to a suspected or confirmed breach.
 - Cultural awareness training.
 - b. Elements related to the results generated by the face recognition system, including:
 - Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.
 - The P/CRCL protections on the use of the technology and the information collected or received, including constitutional protections, and applicable state, local, and federal laws.
 - Face recognition system functions, limitations, and interpretation of results.
 - Mechanisms for reporting violations of Bristol Virginia Police Department face recognition policy provisions.
 - The nature and possible penalties for face recognition policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

9-09: FACIAL RECOGNITION TECHNOLOGY

3. In addition to the training described in N.2, the Bristol Virginia Police Department face recognition examiners are required to complete advanced specialized training to include:
 - Face recognition system functions, limitations, and interpretation of results.
 - Use of image enhancement.
 - Appropriate procedures and how to assess image quality and suitability for face recognition searches.
 - Proper procedures and evaluation criteria for one-to-many and one-to-one face image comparisons.
 - Candidate image verification processes.
4. Investigators from outside agencies are permitted to request face recognition searches from the Bristol Virginia Police Department, only if prior to making requests:
 - There is a formalized agreement, (e.g., a memorandum of understanding or an interagency agreement), between the Bristol Virginia Police Department and the outside agency and the agreement acknowledges that requesting investigators have an understanding of the concepts listed below.
 - The outside agency first provides examples of its applicable policies (e.g., privacy) and acknowledges in writing that its requesting investigators have an understanding of the concepts listed below.
 - There is a law enforcement agency that is making the request based on a valid law enforcement purpose that falls within the authorized uses listed in section A. Purpose Statement, item 3. And, the requestor provides a case number and contact information (requestor's name, requestor's agency, address, and phone number), and acknowledges an agreement with the following statement:

The result of a face recognition search is provided by the Bristol Virginia Police Department only as an investigative lead and IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.

- The agency completes the Bristol Virginia Police Department's training on the following concepts:
 - a. Originating and participating agency responsibilities and obligations under applicable federal, state, or local law and policy.
 - b. P/CRCL protections on the use of the technology and the information collected or received.

9-09: FACIAL RECOGNITION TECHNOLOGY

- c. Conditions and criteria under which the face recognition searches may be requested.
 - d. Face recognition system functions, limitations, and interpretation of results.
 - e. Use of face recognition search results as an investigative lead only.
 - f. Mechanisms for reporting violations of Bristol Virginia Police Department face recognition policy provisions.
 - g. The nature and possible penalties for face recognition policy violations, including dismissal, criminal liability, and immunity, if any.
 - h. Operational policies.
5. In addition to the training described in N.2 & N.3, the Bristol Virginia Police Department requires all personnel who are authorized to run a mobile search to be trained in the following areas prior to utilizing mobile face recognition search capabilities:
- How to capture high-quality face images in the field for most accurate results.
 - The rules and procedures for obtaining an individual's consent to having their image captured.
 - The appropriate use and sharing of information obtained from a face recognition search.
 - The handling of field-acquired probe images including retention and deletion.

Personnel who have not received this training shall not utilize mobile face recognition search capabilities.

O. AGENCY IMPLEMENTATION AND REPORTING REQUIREMENTS

1. Prior to awarding a contract to a Facial Recognition Technology (FRT) vendor or operating its own Facial Recognition program, Bristol Virginia Police Department will submit an email to the Department of General Services (DGS) / Division of Supply and Purchases (DPS) at dpsprocurement@dgs.virginia.gov indicating notice of intent to use FRT. This email will include the name of the vendor (if applicable), prospective implementation date, and the algorithms used by the system (if known). DGS/DPS will notify Bristol Virginia Police Department whether the vendor is approved for state use per § § 15.2-1723.2(B), 23.1-815.1(B), and 52-4.5(B).
2. The Bristol Virginia Police Department will meet state and/or national accreditation standards for the use of Facial Recognition Technology.
3. The Bristol Virginia Police Department shall maintain records regarding its use of facial recognition technology. Such records shall be sufficient to facilitate discovery in criminal proceedings, post-conviction proceedings, public reporting, and auditing of compliance

9-09: FACIAL RECOGNITION TECHNOLOGY

with the Bristol Virginia Police Department's policy. The Bristol Virginia Police Department shall collect data pertaining to:

- a complete history of each user's queries.
 - the total number of queries conducted.
 - the number of queries that resulted in a list of possible candidates.
 - how many times an examiner offered an investigative lead based on his findings.
 - how many cases were closed due to an investigative lead from facial recognition technology.
 - what types of criminal offenses are being investigated.
 - the nature of the image repository being compared or queried.
 - demographic information for the individuals whose images are queried.
 - if applicable, any other entities with which the Department shared facial recognition data.lib
4. In addition to the public posting requirements outlined in §§ 15.2-1723.2(F), 23.1-815.1(F), and 52-4.5(F), the Bristol Virginia Police Department shall enter into an MOU with the Department of Criminal Justice Services (DCJS) assuring the security and non-release of its data. Upon entering into a mutually satisfactory MOU, the Bristol Virginia Police Department will submit FRT use data to DCJS by April 1 of each year following the reporting process and standards outlined in the Facial Recognition Technology Guide for Agency Reporting Requirements. The Data submitted by April 1 should span records queried during the previous calendar year (January through December). The annual posting and the FRT use data shall be retained in accordance with Records Retention and Disposition Schedules promulgated by the Library of Virginia.²
5. Any law enforcement agency who requests a facial recognition query through the Bristol Virginia Police Department must agree to provide use data to the Bristol Virginia Police Department as outlined in the Facial Recognition Technology Guide for Agency Reporting Requirements. Submission of record-level use data for the query is the responsibility of the Bristol Virginia Police Department performing the query. The Bristol Virginia Police Department may decline to run a query for a requesting agency at its discretion. **All requesting agencies must comply with the FRT use policy regarding acceptable use of facial recognition technology query findings**

9-09: FACIAL RECOGNITION TECHNOLOGY

BY ORDER OF

A handwritten signature in black ink, appearing to read 'D. Ashbrook, II', written in a cursive style.

D. BYRON ASHBROOK, II
CHIEF OF POLICE