# Face Recognition Technology

## 343.1 PURPOSE AND SCOPE

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 Department has implemented a face recognition system to support the investigative efforts of department members

It is the purpose of this policy to provide 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.

This policy assists Department and its personnel in:

- Increasing public safety.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Minimizing the threat and risk of damage to real or personal property.
- Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- 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 threat and risk of injury to specific individuals.

## 343.2 POLICY

1. 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

    (a) A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity. For this section, criminal conduct includes violations of criminal state statutes adopted and enforced as a municipal ordinance.

    (b) To support law enforcement in critical incident responses and special events.

(c) To assist in the identification of potential witnesses and/or victims of violent crime.

(d) To investigate and/or corroborate tips and leads.

(e) To assist in the identification of a person who lacks capacity or is otherwise unable to identify him- or herself (such as an incapacitated, deceased, or otherwise at-risk person).

(f) To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.

(g) An active or ongoing criminal investigation.

2. The Department will prohibit access to and use of the face recognition system, including dissemination of face recognition search results, for the following purposes:

(a) Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

(b) Harassing and/or intimidating any individual or group.

(c) 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.

(d) Any purpose that violates the U.S. Constitution or laws of the United States, including the protections of the First, Fourth, and Fourteenth Amendments.

(e) Municipal violations that do not adopt a criminal statute.

(f) Status offenses.

(g) Non-law enforcement (including but not limited to personal purposes).

## 343.3 SYSTEM USE

1. All Department personnel, participating agency personnel, and authorized individuals working in direct support of Department personnel (such as interns), personnel providing information technology services to the Department, private contractors, and other authorized users will comply with the Department's face recognition policy and will be required to complete training in the established FR system prior to use.

2. 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.

3. Department members 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.

4. The 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, establish probable cause, without further investigation. Any possible connection or involvement of the subject(s) to the investigation must be determined through further investigative methods.

## 343.4 OVERSIGHT

1. The Lieutenant or their designee will be responsible for the following:
   (a) Ensuring and documenting that personnel meet all prerequisites stated in this policy prior to being authorized to use the face recognition system.
   (b) Confirming, through random audits, that face recognition information is purged in accordance with this policy and to ensure compliance with applicable laws, regulations, standards, and policy.
   (c) Ensuring that random evaluations of user compliance with system requirements and the entity's face recognition policy and applicable law are conducted and documented.
   (d) Ensuring that user accounts and authorities granted to personnel are maintained in a current and secure "need-to-know" status.
   (e) Acting as the authorizing official for individual access to face recognition information.
   (f) Overseeing and administering the face recognition program to ensure compliance with applicable laws, regulations, standards, and policy.