Facial Recognition Technology

461.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the use of Biometric Facial Recognition Technology.

461.2 POLICY

The policy of the Oxnard Police Department is to utilize Biometric Facial Recognition Technology that allows officers to submit a digital image to the application that will be used to develop investigative leads or the identity of a person. All data and images obtained through the use of facial recognition technology are for the official use of this Department.

461.3 FACIAL RECOGNITION USE

Use of facial recognition technology shall be restricted to officers who have been trained in its use. Training will be given by an authorized trainer designated by the Investigations Bureau Commander or designee.

(a) Facial recognition technology and the use of the applications that facilitate this technology shall only be used for official and legitimate law enforcement business.

(b) Considerations prior to the use of this technology should include whether the individual is lawfully detained and using the facial recognition system does not prolong the detention beyond the time reasonably required to complete the investigation and or contact.

(c) Officers should not typically request facial recognition results when an individual presents a valid driver license or state identification card unless; the officer reasonably suspects the driver license or identification card is forged, altered, or otherwise fraudulent; or the officer reasonably suspects the individual is presenting, as his or her own, a driver license or identification card issued by a DMV to another person.

(d) Department members shall not use physical force to gain compliance during the use, or attempted use, of this technology.

(e) Refusal to submit to the use of this technology does not constitute probable cause for arrest, therefore, no arrests will be made where a subject refuses to submit to the use of this technology without independent probable cause for an arrest.

(f) Prior to any enforcement action based on any results, a peer review or second opinion is highly encouraged when practical. The goal of using facial recognition technology is to generate a strong investigative lead and not to definitively conclude that a face matches an identity.

(g) Any time a subject is arrested and transported to any booking facility, based primarily on an image comparison result, an effort should be made to verify the identity of the subject through the use of additional technology such as fingerprint comparison.

461.4 FACIAL RECOGNITION LIMITATIONS OF USE

Although facial recognition technology can be a remarkably beneficial tool to this Department, it has its limitations. This technology does not provide positive identification, but rather, an investigative lead and analysis to support that lead. The onus still falls on the investigating officer to establish probable cause for arrest by using other investigative means.

461.5 DISSEMINATION OF FACIAL RECOGNITION INFORMATION

Generally and as further outlined below, the Oxnard Police Department may share facial images obtained through facial recognition technology with other government agencies so long as the dissemination is to further the receiving or sending agency's function:

(a) Where it will further a legitimate criminal justice function, the facial images obtained through the use of a facial recognition field identification tool may be shared with other criminal justice agency personnel.

(b) No personally identifying information, including but not limited to mug shot facial images, obtained through the use of facial recognition technology shall be disseminated to members of the general public or news media. This prohibition is subject only to the following specific exceptions:

1. Public Safety Exception - The Investigative Services Bureau Commander or their designee, who reasonably determine that an individual poses a threat of substantial harm to the public, may release the facial images and relevant personally identifying information. The release of facial images and personally identifying information must be limited to information that could reasonably protect the public from harm and the determination to release images must be documented in a report.
2. Photographic Line-up Exception - A suspect’s facial images may be used in a photographic line#up to further the particular investigation for which the suspect’s image was requested.
3. Warrant Exception - Where a warrant has been issued for a known suspect, and where the suspect’s facial image has been verified by an independent witness, the suspect’s facial image can be publicly disclosed for the purposes of locating the suspect or protecting the public.
4. Missing Person Exception - Upon its verification by an independent third#party, the facial image of an individual reported missing can be publicly disclosed to help authorities locate the missing person.

461.6 FACIAL RECOGNITION POLICY REVIEW AND UPDATES

This Department shall regularly review and update this policy and its practices concerning the sharing of facial recognition field identification information to comply with any changes in relevant laws and regulations governing biometric data systems and data sharing**.**