

Handheld Fingerprint Identification

324.1 PURPOSE AND SCOPE

To provide direction for the use of the biometric handheld fingerprint identification devices, more commonly known as a mobile identification device or Mobile ID.

King County's regional AFIS program has initiated a Mobile ID project, involving the use of wireless remote fingerprint identification throughout the county. The project is designed to assist in identifying persons whose identities are in question. While the fingerprint verification process already exists in King County, Mobile ID moves this function to law enforcement first responders, resulting in a more timely identification process. The system scans the fingerprints at the Mobile ID device and transmits wirelessly to the King County AFIS. If the fingerprints are in the AFIS database, a positive match returns the person's specific identifiers to the Mobile ID device or officer's mobile computer. A simultaneous search is also conducted to search Washington State Patrol's AFIS database and an FBI database known as the Repository for Individuals of Special Concern (RISC).

324.2 GUIDELINES FOR USE

Only officers trained and operating under the guidelines of the Mobile ID project may use the device.

In the event that lack of usage by the assigned officer is a concern, the AFIS program will communicate with the agency and provide retraining and/or direct a reassignment of the device.

Any use of the device not consistent with this policy and/or law enforcement purposes may result in reassignment or forfeiture of the device, and/or a deactivation of access to the AFIS database. Additionally, any violation of the Mobile ID policy/procedure, or of federal or state law, may subject the officer to internal discipline by his/her agency.

The use or retention of any Mobile ID-collected data shall conform to federal and state laws. It must also conform to individual agency policy as well as the AFIS program procedure as follows:

- (a) An officer may use Mobile ID when there is probable cause to arrest a suspect.
- (b) An officer may use Mobile ID during an investigative detention (also known as a "Terry Stop") based upon reasonable suspicion of criminal activity. If a person provides a driver's license or other valid means of identification, or gives the officer a name that can be confirmed through a driver's license check, that form of identification should suffice without the use of Mobile ID. However, if there are articulable facts that give rise to reasonable suspicion regarding the accuracy of a person's identity, the officer may use Mobile ID to verify identity.
- (c) Absent probable cause or reasonable suspicion of criminal activity, a person may consent to an officer's request to use Mobile ID. However, the consent must be voluntary as defined by current Washington case law; i.e., the person must be informed that he/she has a right to refuse the officer's request.

Marysville Police Department

Marysville PD Policy Manual

Handheld Fingerprint Identification

- (d) An officer may use Mobile ID as part of a community caretaking function to identify a person when:
 - 1. The person is unable to identify himself/herself because they are deceased, unconscious, physically injured, intoxicated (drugs or alcohol), or suffering from a mental illness or dementia (for instance, Alzheimer's walkaway patient); and
 - 2. The officer does not find any identification; and
 - 3. The officer takes the person into protective custody (for example, under RCW 70.96.120(2) (alcohol), RCW 71.05, 71.34 (mental health), or similar statutes, or to render aid such as having the person transported to the hospital, or to identify and protect an elderly dementia person who is lost.
- (e) Use of the device shall be documented in any report generated as a result of the contact. The officer must articulate the specific facts that support the basis for the use of Mobile ID and must state the voluntary compliance of the Mobile ID if used without arrest, probable cause, or reasonable suspicion.