DALTON POLICE DEPARTMENT

	Effective Date	Number
	September 27, 2011	**GO11- 7.22**
Subject **Rapid ID Digital Fingerprint Device**		
Reference		*Revised* ~~**November 16, 2021**~~ **October 24, 2023**
Distribution **All Personnel**	*Re-evaluation Date* ~~**November 2023**~~ **October 2025**	*No. Pages* **3**

I. Policy

It is the policy of the Dalton Police Department to operate Rapid ID digital fingerprint devices within established guidelines and laws.

II. Definition

Rapid ID Device – A handheld, wireless, two-fingerprint identification solution that searches against a centralized fingerprint database. The database is populated with arrests made in Georgia. The system enrolls four fingerprints, with two fingerprints being used for an identification match. As part of the identification check, automatic secondary searches of wanted files, watch lists, sex offender registries, and probation / parole lists are also included.

III. Procedure

A. Training

1. A Rapid ID device shall only be operated by members that have had documented training on the operation of the unit.

2. Training shall include, at a minimum:

   a. Setup and maintenance procedures

   b. Proper use guidelines

   c. Legal issues surrounding the use of Rapid ID devices

   d. Reporting requirements

   e. The GCIC Terminal Operator Inquiry-level Course

B. Password Protection

Before being authorized to use a Rapid ID device, users shall obtain a unique username and password.

C. Usage Guidelines

1. A Rapid ID device may be used in situations where the subject to be fingerprinted has given a knowing and willing voluntary consent or permission for the member to use the device. This may include consent given during lawful encounters.

   a. As with other forms of consent, the consent can be limited or withdrawn at any point by the subject.

   b. If consent is withdrawn, use of the Rapid ID device is not authorized, and its use must stop immediately. Members shall not force or coerce anyone to submit to the scan.

2. A Rapid ID device may be used in situations where the subject to be printed would otherwise be required to give traditional fingerprints, such as after an arrest for a criminal or traffic offense.

3. Use of the Rapid ID device for random or generalized investigation or intelligence gathering, with no focused case or other legitimate reason, is not authorized.

4. Any specialized, non-standard use of a Rapid ID device shall require notification of and authorization by the Watch Commander or other Supervisor. Examples of non-standard use may include:

   a. A request from an outside agency to fingerprint a suspect in custody. This may be permitted as long as the requesting agency complies with the procedures set forth in this policy.

   b. A death or homicide investigation in which there is no other identifying paperwork for the victim.

   c. To identify an unconscious or otherwise incapacitated subject who cannot be identified by any other means.

5. Guidelines cannot be written to encompass every possible application for the use of a Rapid ID device. Members, therefore, shall consider the guidelines set forth in this policy to assist them in deciding whether the device may be used or not.

6. Members are expected to be able to justify, based on these guidelines, training, experience, and assessment of the circumstances, how they determined that use of a Rapid ID device was justified.

7. Supervisors shall directly monitor the usage of the Rapid ID device.

D. Documentation

Each time the Rapid ID device is utilized, the user shall document the occurrence in an incident report, regardless of whether or not an identification is made of the subject that was scanned. Each report shall include the circumstances leading up to the usage of the device and any actions taken as a result.

This policy supersedes any previous policies issued.

BY ORDER OF

_____

CHIEF OF POLICE