"Keep Orlando a safe city by reducing crime and maintaining livable neighborhoods."

ORLANDO POLICE DEPARTMENT POLICY AND PROCEDURE

1642.0, USE OF DAVID

EFFECTIVE DATE:	9/20/2023
RESCINDS:	WD 18-03
DISTRIBUTION GROUP:	ALL EMPLOYEES
REVIEW RESPONSIBILITY:	INTELLIGENCE UNIT COMMANDER
ACCREDITATION STANDARDS:	N/A
RELATED LAWS:	Fla. Stat. 943.0525, Fla. Stat. 119.0712(2), U.S Code 18 U.S.C. 2721
RELATED POLICIES:	P&P 1637
CHIEF OF POLICE:	ERIC D. SMITH

CONTENTS:

1. PURPOSE

The purpose of this policy is to establish procedures for member use of the Driver and Vehicle Information Database (DAVID) systems. The D.A.V.I.D system is an extremely helpful law enforcement tool to be used exclusively for official law enforcement investigations. The system is routinely audited, and the users must comply with the D.A.V.I.D Usage Agreement. The unauthorized use of D.A.V.I.D is a violation of the "Driver Privacy Protection Act" (U.S. Code 18 U.S.C. 2721) and may be pursued as a civil rights and/ or criminal violation with costly punitive damages.

2. POLICY

The Orlando Police Department Intelligence Unit regulates the Driver and Vehicle Information Database (DAVID). The system shall only be used to obtain information for legitimate law enforcement purposes. Information obtained through the system shall not be shared or released to unauthorized persons. Only personnel who have been granted access, received applicable training, or are in a training status under the guidance of a trainer, may access the above system. The entering and retrieval of information shall be in accordance with the rules and procedures established by DHSMV. Any suspicious activity regarding an agency employee shall be forwarded to Internal Affairs.

3. DEFINITIONS

DAVID: The Driver and Vehicle Information Database system that accesses and transmits driver and vehicle information.

Driver License Information: Driver license and identification card data collected and maintained by the Department of Highway Safety and Motor Vehicles (DHSMV). This information includes personal information as defined below.

Driver Privacy Protection Act (DPPA): The Federal Act (see, 18 United States Code§ 2721, et seq.) that prohibits release and use of personal information except as otherwise specifically permitted within the Act.

Emergency Contact Information (ECI): Information contained in a motor vehicle record listing individuals to be contacted in the event of an emergency. Emergency contact information may be released to law enforcement agencies through the DAVID system for purposes of contacting those listed in the event of an emergency, as noted in Section 119.0712 (2)(d), Florida Statutes.

Government Entity: Any non-law enforcement agency of the state, city or county government and all Federal agencies, which may include Federal law enforcement agencies.

Insurance Record: Insurance information, such as Insurance Company name, policy type, policy status, insurance creation and expiration date provided to the Requesting Party, pursuant to Section 324.242(2), Florida Statutes.

Personal Information: As described in Chapter 119, Florida Statutes, information found in the motor vehicle record, which includes, but is not limited to, the subject's driver identification number, name, address, telephone number, social security number, medical or disability information, and emergency contact information.

Point-of-Contact (POC): A person(s) appointed by the Orlando Police Department as the administrator of the DAVID program.

Providing Agency: The Florida Department of Highway Safety and Motor Vehicles. The Providing Agency is responsible for granting access to DAVID information to the Requesting Party.

Quarterly Quality Control Review Report: Report completed each quarter by the Requesting Party's POC to monitor compliance with the MOU.

Requesting Party: Any law enforcement agency that is expressly authorized by Section 119.0712(2), Florida Statutes, and DPPA to receive personal information contained in a motor vehicle record maintained by the Providing Agency.

Vehicle Information: Title and registration data collected and maintained by the Providing Agency for vehicles.

4. PROCEDURES

4.1 AUTHORIZED USE

To ensure compliance with the FBI CJIS Security Policy and all related rules, regulations, policies and procedures established for DAVID and related networks, only documented, authorized personnel shall be granted access to the various criminal justice information systems; all such authorized users, to include contract law enforcement agencies and its authorized personnel, shall be bound by the security requirements as set forth in the User Agreement with the

Florida Department of Law Enforcement (FDLE) and Orlando Police Department Policy 1637, Criminal Justice Information Services (CJIS) Security.

Due to the sensitive nature of the data available on hardware devices and software programs and the associated links with other systems, the following guidelines shall be adhered to:

a. No information shall be obtained for the personal gain of the user or their acquaintance. Any use shall result in disciplinary action up to and including termination and/or criminal prosecution.
b. The transfer of confidential information, intelligence files, and other sensitive materials from agency computers or Personal Communications Devices to non-agency computers, Personal Communications Devices, or unauthorized persons, whether in electronic or printed format, is strictly prohibited.
c. Information obtained through computer interfaces to other state or federal systems (e.g., DAVID), by means of access granted pursuant to F.S.S. 943.0525, can only be used for criminal justice purposes and shall only be accessed by authorized users. Users of DAVID shall adhere to all policies, procedures, and operating instructions contained in the FBI CJIS Security Policy and all related rules, regulations, and technical memoranda published by FDLE.

Access to ECI within DAVID is dictated by F.S.S. 119.0712(2)(d)2 and limits access to law enforcement officials in order to locate and contact family members in the event of an emergency involving the provider of the information.

- The Florida Legislature has limited the release of ECI "to law enforcement agencies for purposes of contacting those listed in the event of an emergency". The emergency must involve the person who submitted the information to DHSMV.
- ECI shall only be used for the purpose of notifying a person's registered emergency contact in the event of a serious injury, death, or other incapacitation. ECI shall not be released or utilized for any other purpose, including developing leads or for criminal investigative purposes.
- Contact the DAVID POC if necessary for ECI access.

Any individual who becomes aware that a user has misused personal information obtained from the DAVID system, shall notify Internal Affairs.

a. The Internal Affairs Investigator is responsible for notifying the agency Point of Contact (POC) for DAVID.
b. The POC is responsible for following their instructions regarding notification to the individual(s) whose personal information has been compromised, at the conclusion of the Internal Affairs investigation.
c. The POC is responsible for the notification to the appropriate network administrator and shall include the date, and number of records affected.
d. DAVID violations shall also include:
    1. Information regarding the notification of the affected individual.
    2. Corrective actions.
    3. Date of actions completed.

4.1.1 QUALITY CONTROL AND AUDITS

Ongoing reviews of agency use of the DAVID system shall comply with the current Memorandum of Understanding (MOU) with the DHSMV.

All access to the DAVID system shall be monitored on an ongoing basis. To ensure the authorized use and dissemination of DAVID information, the DAVID System POC or designee shall conduct the following audits:

a. An audit, once every two years as instructed by the DHSMV. The Chief of Police shall be notified of the audit results and be provided an attestation form from DHSMV.
b. Quarterly audits by reviewing a sampling of agency members with DAVID access.

1. Member's suspicious DAVID activity discovered as a result of the audit, shall be forwarded to the member's supervisor for review.
2. Suspected misuse of the DAVID system shall be investigated pursuant to Policy 1604, Discipline, and the current collective bargaining agreement.

c. Individual audits will be conducted for any activity that appears suspicious or the POC is notified by DHSMV or Internal Affairs of a civilian complaint or suspicious activity.
d. Additional procedures shall be included and utilized as directed by DHSMV.

4.2 TERMINAL SECURITY

Terminals accessing DAVID are required to be physically placed in secure locations. Terminal operators must be screened and access to the terminal is restricted. Operators must adhere to all provisions of the FDLE User Agreement:

a. Members are required to treat DAVID information as sensitive and ensure that the information displayed on terminal screens and information printed from terminals is not visible to un-authorized persons.
b. Any person who may come in contact with sensitive information shall follow current CJIS security awareness guidelines.
c. Authorized users with assigned Agency vehicles equipped with MCT's shall close the lid of their computer when exiting the vehicle with the computer on to prevent non-CJIS certified members or citizens from viewing data on their screen.

Agency policy mandates that Communications Division personnel use a secured method to access the DAVID database. Concurrent sessions of DAVID, whether initiated on a single device or multiple devices, is prohibited.

4.3 DRIVER AND VEHICLE INFORMATION DATABASE (D.A.V.I.D)

All data contained within the DAVID system is sensitive and privileged information and shall be handled accordingly. To maintain the integrity of this information, the records shall be accorded proper management and security, and shall only be accessed and used by authorized personnel in accordance with state and federal law.

Activity associated with any aspect of the DAVID system is subject to detailed monitoring and audits to protect against improper or unauthorized use. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use including looking up personal information, dissemination, sharing, copying or passing of DAVID information to unauthorized users. Unauthorized use could result in civil proceedings against the agency and/or civil or criminal proceedings against any user or other person involved. Violations or misuse may also subject the user and the agency to DHSMV administrative sanctions, disciplinary action against the user, and possible DAVID access termination.

Computers with access to DAVID shall not be left unattended without enabling a password-protected screen saver or logging off the computer entirely. If a user suspects that their password has been compromised, the user should immediately update the password and immediately notify one of the agency DAVID POC.

The agency's POC for DAVID shall maintain a list of current users and ensure proper notifications are made when a user has been deactivated in the system.

The Orlando Police Department has signed a Memorandum of Understanding (MOU) with the Florida Department of Highway Safety and Motor Vehicles (DHSMV) for access to DAVID. Information obtained from DAVID can only be disclosed to persons to whom disclosure is authorized under F.S.S. 119.0712(2), and federal law (Driver's Privacy Protection Act, 18 U.S.C. s. 2721-2725).

4.4 DAVID UTILIZATION

DAVID use shall be restricted to agency computers and Personal Communication Devices of approved users only. Any employee authorized to access DAVID must do so for legitimate law enforcement purposes and shall choose the appropriate purpose code within the system to articulate a reason for making any inquiries.

5. FORMS AND APPENDICES

N/A