
	Florida State University Police Department	
Driver and Vehicle Information Database (DAVID)		
Revision Effective Date: 09/05/17	General Order 1105	Attachments: <i>Administrative Bulletin # A2013-001: "Use of Emergency Contact Information in DAVID"</i>
Rescinds/Amends: 14-33D (8/8/14, 6/3/14)	Distribution: Department Wide	CFA Reference: None
	Pages: 7	

POLICY - Driver and Vehicle Information Database (DAVID)

This general order will establish agency policy and procedure for access and usage of the state Driver and Vehicle Information Database (DAVID). The DAVID system provides important personal information, vehicle information, and photographs useful for criminal investigations and for other law enforcement - related purposes. The database may be accessed through the internet by use of a secure user name and password established by the employee upon initially accessing the DAVID system.

Driver's license and vehicle record privacy laws form the basis for this policy. To adequately provide the user clear information, this general order will establish the application of these laws to the tasks performed in the agency.

This general order is based on the provisions of the Memorandum of Understanding (MOU) form issued by FDHSMV, dated 6/12.

A. PROCEDURE

Agency personnel accessing and using information obtained from the state Driver And Vehicle Information Database (DAVID) will comply with the Driver's Privacy Protection Act (18 United States Code, Title 1, Chapter 123, Section 2721 et seq. and F.S. 119.0712.) and the information safeguards stated in the Memorandum of Understanding (MOU) executed with the Florida Department of Transportation, Division of Highway Safety and Motor Vehicles (FDHSMV) as outlined in this general order.

Information obtained under the provisions of the MOU will only be disclosed to authorized under Florida law and federal law.

B. ACCESS to DAVID

1. Access to the DAVID system will be available upon request, to agency personnel where a reasonable investigative or administrative need for Florida driver's license and/or vehicle registration information exists. This would include, but not be limited to sworn members,

crime analysis personnel, and Communications personnel. Other personnel may be permitted access upon approval of his/her supervisor.

2. Access is limited to FSU Police Department owned or issued computer equipment and computer equipment provided for law enforcement use at the Leon County Jail or other law enforcement agencies.
3. Users will not be authorized to access DAVID using the username and password of another individual.

C. SYSTEM ADMINISTRATION

The DAVID Point of Contact (POC) will ensure appropriate internal controls are implemented and maintained which protects personal data obtained through DAVID from unauthorized access, distribution, use, modification, or disclosure.

1. The chief shall appoint an Agency Point of Contact for the DAVID system. The POC(s) shall be responsible for approving additional users, removing users, and conducting required audits.
2. The DAVID POC(s) will:
 - a. Approve and assist personnel in obtaining access to the system at the agency level.
 - b. Update user access permissions upon termination or reassignment of users within five working days and immediately update user access permissions upon discovery of negligent, improper, or unauthorized use or dissemination of information.
 - c. Ensure compliance with the terms of the MOU and applicable laws by ensuring compliance with this general order.
 - d. Ensure the required forms are completed and submitted.
 - e. Monitor access to the information and conduct documented quarterly quality control reviews.
 - f. Cooperate with any external audits ordered by the agency or FDHSMV.
 - g. Send an annual affirmation indicating compliance with the requirements of this agreement no later than 30 days after the anniversary date of this agreement. The form or format as provided by FDHSMV will be used, if provided. This should be included with the annual attestation. (Audit)
 - h. Report misuse to FDHSMV.
 - i. Create and administer training for new DAVID system users.
 - j. Ensure that all pertinent documentation is adequately retained.

D. AUTHORIZED USE OF DAVID INFORMATION

Consistent with 18 United States Code, Title 1, Chapter 123, Section 2721 et seq. and F.S. 119.0712, DAVID information may be used for:

1. Criminal and traffic investigations.
2. Distribution of photographs of missing persons (adults or children) to the public to aid in their recovery.
3. Investigation of child neglect, not necessarily criminal.

4. Agency employment driver's license background checks or status checks.
5. Agency internal investigations of DAVID misuse or to aid in internal investigations.
6. Verification of identity or background checks for agency volunteers or contractors.
7. Providing notice to the owners of towed or impounded vehicles.

E. Emergency Contact Information (ECI)

The Emergency Contact Information program was enacted so there is little delay in notifying concerned relatives or emergency contacts in the event a license holder is killed or seriously injured.

Emergency Contact Information is confidential and may only be accessed in the event of an emergency as listed below:

1. The licensee has serious bodily injury or has been killed in a traffic crash
2. The licensee has serious bodily injury or has been killed as the result of a natural disaster
3. The licensee is involved in a confirmed missing person's incident
4. The licensee is being or was transported to the hospital by ambulance and is not capable of notifying anyone, i.e. unconscious, impaired or as the result of a Baker or Marchman Act.

The Emergency Contact does not have to be contacted in order for their information to be considered "accessed." If a Department member feels a condition exists as a result of one of the above incidents that they need Emergency Contact Information, they may request it from a patrol supervisor, a member of command staff or an investigator. If ECI is accessed, it must be documented in the associated Spillman report as to why it met the required criteria, and if the Emergency Contact was notified.

Since FSUPD officers do not utilize Spillman at the Panama City Campus, if the ECI is accessed by a patrol supervisor, a member of command staff, or an investigator, (approved individual) at the Panama City Campus, the approved individual is required to click the "other" box when prompted for the reason for the access. The approved individual is required to state in the "other" box the specific reason for accessing the emergency contact information.

F. SECURITY OF INFORMATION

Agency personnel and authorized users will:

1. Not retain DAVID records (including photos), except as required as part of an official report.
2. Not provide DAVID records to any third party. (Note: FDHSMV does not consider the courts and SAO as a third party).
3. Protect access to the information obtained in such a way that unauthorized persons cannot review or retrieve the information.
4. Minimize or close any computer screen when any unauthorized person is within viewing range of secure information.
5. Not interface DAVID to a "third party."

6. Be permitted to use DAVID photos for photo line-ups. The photo may be copied and pasted into a paper document for use as a photo line-up. The paper photo line-up shall become part of the official case file after it has been used. Members are prohibited from keeping digital copies of DAVID photos stored on any other medium outside of the DAVID system.

G. DRIVER'S PRIVACY PROTECTION ACT (DPPA) AND PUBLIC RECORDS ACCESS

1. Unauthorized Use and Release

Information obtained from the DAVID system will not be used for any purposes not specifically authorized by this general order (consistent with the MOU). Unauthorized use includes, but are not limited to, queries not related to a legitimate business purpose, personal use, and the dissemination, sharing, or providing of DAVID information to unauthorized persons.

2. Release of Information

Agency personnel and authorized users will protect and maintain the confidentiality and security of personal information from driver's licenses, motor vehicles, and traffic crash records received from DAVID in accordance with the MOU and applicable state and federal law. Information obtained from the DAVID for criminal investigative purposes and criminal intelligence (normally exempt and confidential under F.S. 119.071) may only be released:

- a. In the furtherance of official duties and responsibilities, including apprehension of suspects.
- b. For print, publication, or broadcast if the agency determines that such release would assist in locating or identifying a missing or endangered person. The information provided should be limited to that needed to identify or locate the victim and not include the sexual nature of the offense committed against the person.
- c. To another governmental agency in the furtherance of its official duties and responsibilities. All other public records request for DAVID information will be referred to the originator of the records, the Florida Department of Motor Vehicles.

H. User Acknowledgements

All DAVID users shall read and sign this General Order and Administrative Bulletin #A2013-001: "Use of Emergency Contact Information in DAVID" in the Power DMS (Document Management System), acknowledging:

1. The confidential nature of the DAVID information.
2. The criminal sanctions specified in state law for unauthorized use of the data.

I. DAVID PROCEDURE

1. Agency members/employees needing access to DAVID for official use will contact the DAVID POC(s), providing the purposes for use and access.

2. Upon approval, the DAVID POC(s) will either enroll the employee or send him/her a self-registration link to the DAVID system whereby the employee may complete the registration process. The POC(s) shall then, after receiving notice that an application is awaiting approval, verify that all information entered by the employee is accurate.
3. Upon approval of the application and after the user's account is set up including the level of access, the user will be notified of their user number and temporary password. The user will then follow the instruction on establishing a permanent password and complete the FDHSMV required training before gaining full access to the DAVID system.
4. The POC(s) shall ensure that the employee has read this general order.
5. All DAVID users are required to sign a new criminal sanctions and confidential information acknowledgement (*Administrative Bulletin #A2013-001: "Use of Emergency Contact Information in DAVID"*) in the Power DMS system every 12 months. The DAVID POC(s) will make a user's access INACTIVE if the user does not complete the criminal sanctions and confidential information acknowledgement within 30 days of the anniversary date of the previous signing.
6. When assistance is required, the member/employee should the DAVID POC(s).
7. Documentation generated from the DAVID system will be destroyed when no longer useful, if not placed in official files.
8. When using computers, particularly laptop computers, with DAVID access, members/employees will ensure that non-releasable highly sensitive personal information is not visible to the public.
9. Members/employees will immediately report misuse of DAVID personal information to the DAVID POC(s).

J. **TRAINING**

New users will receive training upon gaining access or prior to accessing DAVID records. Training may be conducted using a field training method or on-line. The training will be designed to ensure the user operates the system properly and understands the privacy safeguards. A review of this general order will be included in the training.

If the terms of the MOU or user guidelines in this general order are changed, a new annual acknowledgment will be signed by each user. Notification and or training, if necessary, will precede the acknowledgement.

K. **MISUSE**

Misuse of personal information must be reported to the DAVID POC(s) who must immediately notify the Chief of Police. The Chief shall determine if the report should be investigated by the POC(s) or if it should be turned over to the Internal Affairs Officer for investigation. At the close of the investigation, FDHSMV shall be notified pursuant to the requirements of the MOU.

L. **QUALITY CONTROL AND AUDITS**

1. Quarterly quality control reviews will be conducted and will focus on ensuring that all current users are appropriately trained, authorized to use the system, and have a current acknowledgement form on file. This may be accomplished by comparing the list of authorized users with a list of personnel reassigned or terminated since the prior review.

The reviewer will ensure that FDHSMV has been requested to revoke the site certificate of former users. An agency form will be prepared for the review within 30 days of the end of the quarter.

2. The Communications Section Manager/designee will review the site certificate list (via the shortcut) for the Communications Section at the end of each quarter to ensure the list accurately reflects authorized users. (Terminated or transferred personnel should not appear on the user lists.) A form indicating the review has been completed with any corrective actions needed/completed will be submitted within 10 business days to the DAVID POC(s) for inclusion with the quarterly quality control review.
3. Human Resources personnel will include DAVID POC(s) in all notifications of all personnel terminated or reassigned.
4. The Internal Affairs Officer will conduct an annual audit within 30 days after the anniversary date of the MOU to ensure proper and authorized use and dissemination.
5. The audit must be sufficient enough to allow the auditor to attest that internal controls of the personal data are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure.

The audit will consist of:

- a. A compilation of the quarterly quality control reviews.
- b. A summary of any incident reports, memorandums, or other documentation related to system misuse or improper disclosure of information.
- c. A review of this general order for needed updates, such as may be necessary due to amendments to the MOU, organizational changes, or other operational changes.
- d. Observations of non-compliance with the related written directives.
- e. A check of site certificates on randomly selected agency computers.

The completed annual audit will be forwarded to the Administrative Services Bureau Commander for Review and approval. Upon approval, the auditor will sign an attestation in a format or on a form provided by FDHSMV.

The audit and the attestation will be provided to the DAVID POC(s) who will submit the attestation to FDHSMV.

6. Additional procedures will be included as directed by FDHSMV.

Glossary

DRIVER AND VEHICLE INFORMATION DATABASE (DAVID) – A driver’s license and vehicle registration database maintained by the Florida Department of Transportation Division of Highway Safety and Motor Vehicles.

DRIVER’S PRIVACY PROTECTION ACT (DPPA) – United States Code regulating the use of driver’s license information. (18 United States Code section 2721 et seq.)

FLORIDA DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES (FDHSMV) – State agency responsible for computerized driver’s license, vehicle, and traffic crash records. For purposes of this general order, FDHSMV is the “provider agency” for DAVID information.

HIGHLY RESTRICTED PERSONAL INFORMATION - An individual's photograph or image, social security number, medical or disability information. (DAVID MOU definition.)

DAVID SYSTEM POINT OF CONTACT (POC) – Agency member(s) or employee(s) designated by the Chief to manage and supervise the DAVID system at the agency level.

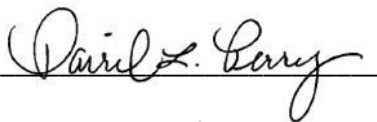
PERSONAL INFORMATION – Information found in the motor vehicle or driver record which includes, but is not limited to, the subject's driver identification number, name, address, telephone number, and medical or disability information. Personal information does not include information related to vehicular crashes, driving violations, and driver's status. (18 USC S.2721 definition.)

Index

DAVID
DAVID System
Driver and Vehicle Information Database
Emergency Contact Information
ECI

Attachments

Administrative Bulletin # A2013-001: "Use of Emergency Contact Information in DAVID"

MTC 09/05/17 Filed: General Order 1105
Title: Driver and Vehicle Information Database (DAVID)
Approved: 
David L. Perry, Chief
Date: 09/05/17