Data Extraction Device Policy

610.1 PURPOSE

The purpose of this policy is to assist members in the training, usage, and maintenance of data extraction device (DED's). This policy applies to all KDPS personnel and those assigned to KDPS supervised work units authorized and trained to use a DED.

610.2 POLICY

1. DED's shall be used in accordance with all state and federal laws pertaining to search and seizure of digital media.

2. The incident report shall include a description of the device, the model and serial number of the device analyzed. If the owner of the phone is known it should be included in the report. Additionally the following, as applicable shall apply:

   (a) Either verbal consent, written consent or a search warrant authorizing the analysis of the device as an external document.

   (b) If an exception to the search warrant rule is the basis of the search, the exception used as well as factors supporting the exception shall be noted in the incident report.

   (c) If verbal consent is the basis of the search, the investigating officer obtaining the verbal consent shall be noted in the incident report, along with the name of the person authorizing consent, the date and time consent was given and articulation of the authority of that person to grant consent.

3. Only personnel trained by certified DED examiners are permitted to operate DED's.

4. DED users are required to complete a data extraction report any time an extraction is completed on a device. If an extraction was attempted but not successful it should be documented in the incident report.

5. The Captain of CID or his/her designee shall be able to produce saved records of the device upon request by the Chief or his/her designee or through FOIA.

610.3 EVIDENCE FILES

CID is responsible for maintaining the DED and shall ensure there is dedicated external storage media to be used to hold digital evidence files obtained from the target devices. At the time an extraction is made, this recovered data shall be archived to another device and maintained as manufactured evidence.

610.4 SOFTWARE LICENSING

CID is responsible for keeping the licensing and software current. The Captain of CID shall be notified any time the device is upgraded or taken out of service.