On October 30, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following Cellebrite Universal Forensic Extraction Device (CUFED) Use Policy (26.07.030 Davis Municipal Code)

**Surveillance Use Policy**

(a) **Purpose:** The specific purpose(s) that the surveillance technology item is intended to advance.

The CUFED is used to extract data from cell phones, smart phones or PDA’s for use in criminal investigations.

(b) **Authorized Use:** The uses that are authorized, and the rules and processes required prior to such use.

The CUFED will be used to extract data from cell phones, smart phones or PDA’s during criminal investigations via search warrant, written owner consent or when command staff has determined that exigent circumstances exist and that data must be extracted without delay (in these cases, a search warrant shall be secured within 3 days following the search as required by California Penal Code Part. 2, Title 12, Chapter 3.6).

(c) **Data Collection:** The information that can be collected by the surveillance technology, including “open source” data.

Data includes:

- Device Information – Phone Number, IMEI, IMSI, MEID, ESN & MAC ID (identifying device info.)
- Phonebook – Contact Name and Numbers
- Call Logs
- Text and Picture Messages
- Videos and Pictures (in some cases with GeoTag-location info) and creation date and time
- Audio Files
- Emails and Web Browsing Information (in some devices)
- GPS and Location Information (in some devices)
- Social Networking messages and contacts (in some devices)
- Deleted Data – Call Logs, Messages, Emails (in some devices)
- PIN Locked and Pattern Locked Bypass & Data Extraction – (on some devices – not all phones bypassed)
- Attached Media or memory card extraction (Pictures, files, app data – located on media card)
- Wireless (WI-FI) networks connected to the device (can assist in localizing a phone to a specific area)
(d) **Data Access:** The category of individual who can access or use the collected information, and the rules and processes required prior to access or use of the information.

The CUFED can only be used by authorized police department personnel who are trained in its use and with approval of command staff when authorized by state and federal law.

(e) **Data Protection:** The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms. Nothing in this subsection shall be construed to require the disclosure of information that could reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of the City.

Data gathered by the CUFED is stored on a secure department server by downloading to a connected desktop computer. Data can then be printed hardcopy, loaded to a portable drive or burned to disc. All data is protected by password. The CUFED is secured in a locked area within the police building while phones and devices awaiting inspection are stored in the secured evidence room.

All downloaded and retained media shall be treated in the same manner as other evidence. Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

(f) **Data Retention:** The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.

Extracted data is attached to criminal investigations. Records related to criminal investigations are kept for statutorily varying periods depending on the type of record, whether a person has been prosecuted and/or whether the record has been lawfully sealed. Records that are no longer needed will be destroyed in accordance with laws relating to the destruction of evidence when it is no longer needed or as required by the Electronic Communications Privacy Act or court order.

(g) **Public Access:** How collected information can be accessed or used by members of the public, including criminal defendants.

All data is for the official use of the Davis Police Department.

Requests for data from the public or the media shall be processed in the same manner as requests for department public records.

Members of the public do not have access to this information when it is gathered as part of a criminal investigation; it is exempt from public disclosure pursuant to a public records request.
Data that is the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

Criminal defendants have access to information pursuant to state and federal laws relating to discovery. Discovery is overseen by the courts.

(h) Third Party Data Sharing: If and how other City or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information. Extracted data is generally only used by the Davis Police Department. However, extracted data may be shared with other law enforcement agencies who are involved in a joint criminal investigation, or who are conducting their own criminal investigation. Sharing data requires authorization from command staff. Data can also be shared with various prosecutors’ offices, including District Attorney’s, State Attorney or United States Attorney, as well as with criminal defendants and their attorneys through the criminal discovery process or as otherwise required by law.

(i) Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology. Individuals who operate the CUFED are trained in its use by department trainers and may also receive training directly from the vendor.

(j) Auditing and Oversight: The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy. The use of the device is documented in a criminal police report. These devices are stored at the police department when not in use. A member is subject to discipline for unauthorized use or misuse.

The Police Chief or the authorized designee will conduct an annual review of the use of the device. The review should include an analysis of the cost, benefit and effectiveness of the device, including any public safety issues that were effectively addressed or any significant prosecutions that resulted, and any systemic operational or administrative issues that were identified, including those related to training, discipline or policy.

The results of each review shall be appropriately documented and maintained by the Police Chief or the authorized designee and other applicable advisory bodies. Any recommendations for training or policy will be promptly addressed.

Darren Pytel
Police Chief
October 30, 2018