On October 30, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following GPS Tracker Device 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.

Improve public safety by providing an effective method of investigating criminal activity. GPS trackers can be used to track items instead of using human surveillance. This is a cost effective way to investigate crime.

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

GPS tracking devices can be used during criminal investigations and ‘bait” type operations. GPS tracking devices will be used by sworn peace officers. Use of the devices must be authorized by a supervisor or manager and a warrant or waiver is required for non-bait surveillance operations.

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

Devices use Global Positioning System (GPS) technology to track the location of the device by longitude and latitude. The information gathered by the device includes geographic location (Latitude/Longitude), time, speed and direction. The information is not open source and is only accessible by the account holder and vendor.

(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 information will be accessed by law enforcement officers during an investigation and court process. If the information is included as evidence in a criminal case, the information will be accessed by the prosecuting attorney and the defense attorney through the discovery process. The service vendor is bound by strict requirements that they may not share any information collected by the Davis Police Department.

(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.

GPS tracking device accounts require an account administrator be assigned by the agency using their product. The administrator assigned at the Davis PD for administrating GPS tracking device accounts is the Investigations Division Sergeant and/or lieutenant. The
account administrator has the ability to assign “users” who have the ability to change certain settings on the device and make reports, or assign individuals the ability to “view only”, which limits access to only logging in and viewing real time data. The account administrator can also assign passwords, change passwords and delete data.

(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.

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 court order.

Any data that is not attached to a criminal case is deleted.

(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 or as otherwise required by law. 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.

Data is generally only used by the Davis Police Department. However, 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.

GPS Device users are trained by other officers on how to use the device and obtain the data.
(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 a 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 devices. 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