On October 30, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following Covert Personal Recording Devices 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 tool used to record undercover or covert police operations.

(b) Authorized Use: The uses that are authorized, and the rules and processes required prior to such use.
   Covert Personal Recording Devices will be used for undercover operations during criminal investigations and will be used or monitored by sworn peace officers. Use of the devices must be authorized by a supervisor or manager.

   Equipment shall not be used in an unequal or discriminatory manner and shall not target protected individual characteristics including, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation.

   Equipment shall not be used to harass, intimidate or discriminate against any individual or group.

(c) Data Collection: The information that can be collected by the surveillance technology, including “open source” data.
   Covert Personal Recording Devices record voice conversations or video images. The data is not open source and is stored on a vendor secure server.

(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.

   All downloaded media shall be stored in a secure area with access restricted to authorized persons. A recording needed as evidence shall be copied to a suitable medium and booked into evidence in accordance with established evidence procedures. All actions taken with respect to retention of media shall be appropriately documented.
(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.

Information gathered by Covert Personal Recording Devices can be stored in one of two ways. Devices that are simply recording to a receiver that is controlled by the investigating officer, generally stores the information on the device and later downloads it onto a secure police evidence server. Devices that require vendor support generally keep information stored on the vendors secure servers.

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.

The type of video surveillance technology employed and the manner in which recordings are used and stored will affect retention periods. The recordings should be stored and retained in accordance with the established records retention schedule and for a minimum of one year. If recordings are evidence in any claim filed or any pending litigation, they shall be preserved until pending litigation is fully resolved.

Recordings are generally 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.

Any recordings needed as evidence in a criminal or civil proceeding shall be copied to a suitable medium and booked into evidence in accordance with current evidence procedures. Records that are no longer needed will be destroyed in accordance with laws relating to the destruction of evidence or by court order.

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

All recordings are for the official use of the Davis Police Department.

Requests for records 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 recordings when they are gathered as part of a criminal investigation; it is exempt from public disclosure pursuant to a public records request.
Recordings that are 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. Information gathered by Covert Personal Recording Devices may be shared with other law enforcement agencies who are involved in a joint investigation, or who are conducting their own investigations. Information can also be shared with various prosecutors’ offices, including the District Attorney, State Attorney or United States Attorney. Recordings may also be shared with defendants and their attorneys through the discovery process, as established by state and federal law and overseen by the courts.

(i) Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology. All department members authorized to operate a Covert Personal Recording Device shall receive appropriate training. Training will include guidance on the use of the devices, interaction with dispatch and patrol operations and a review regarding relevant policies and procedures, including this policy. Training will also address state and federal law related to the use of video surveillance equipment and privacy.

(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. Covert Personal Recording Devices must be authorized by a police sergeant, lieutenant or other sworn administrator. Use of these devices for criminal investigations is documented in the police report. Devices are stored at the police department or other law enforcement facility while 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 use of the devices. The review should include an analysis of the cost, benefit and effectiveness of the system, 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 should be promptly addressed.

Darren Pytel
Police Chief
October 30, 2018