On October 30, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following Remote Public Safety Cameras 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.
   To provide remote video observation in designated public locations.

   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.

(b) Authorized Use: The uses that are authorized, and the rules and processes required prior to such use.
   Remote cameras will be used to monitor certain city events where there are large crowds, provide remote surveillance for areas where criminal activity is occurring and of subjects suspected of being involved in criminal activity.

(c) Data Collection: The information that can be collected by the surveillance technology, including “open source” data.
   Remote cameras can collect still images and record video. The images and video are not open source data and are stored to an internal DVR on the individual camera.

(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 video and/or images may 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 remote cameras can be stored to an internal DVR and then saved
onto a removable drive. Video/images gathered as part of a law enforcement investigation are
saved by the investigating officer and saved to a secure police evidence server.

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.

In those cases where the video is part of a criminal or civil investigation/litigation, the video
must be kept for a period of at least two years or until it is no longer needed for litigation.

The Police Chief may destroy recordings of routine video monitoring after one year.

Routine video monitoring may also be destroyed after 90 days if a written log is kept of the
recording.

Most video falls within the 90 day retention period meaning that only a written log of what
was recorded is kept. In those cases where the video has something of evidentiary value, it
will be kept for at least 2 years or until any litigation has been resolved.

(g) Public Access: How collected information can be accessed or used by members of the
public, including criminal defendants.
All recorded video images gathered by the cameras are for the official use of the Davis Police
Department.

Requests for recorded video images 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.

Requests for recorded images from other law enforcement agencies shall be referred to the
Police Chief for release in accordance with a specific and legitimate law enforcement
purpose.

Recorded video images 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.
Images gathered by remote cameras may be shared with other law enforcement agencies who are involved in a joint investigation, or who are conducting their own investigations. Images may also be shared with various prosecutors’ offices, including District Attorney’s, State Attorney or United States Attorney, as well as with defense attorneys through the discovery process when they are evidence.

(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 or video shall receive appropriate training. Training will include guidance on the use of cameras, 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 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.
Remote cameras must be authorized by a police sergeant, lieutenant or other sworn administrator. Use of these cameras for criminal investigations is documented in a police report. These 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 the public safety video surveillance system. 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 will be promptly addressed.

Darren Pytel
Police Chief
October 30, 2018