BP 3516 Video Surveillance

PURPOSE OF Video Surveillance at school

The primary purposes of having a video surveillance system in our schools are for student and staff safety, the deterrence of staff and student behavior that (does not support the education mission of the school), including incidents of bullying, criminal activity, school thefts and break-ins, etc.

Deterrence: The primary objective of PSD in acquiring or deploying a video surveillance system is the prevention of crime and student misconduct. The acknowledged presence of security cameras in appropriate locations provides a disincentive for illegal or inappropriate behavior, and helps ensure a facility is safe for students, staff, and visitors.

Apprehension: A secondary objective of video surveillance deployment is to facilitate the apprehension of those that will not be deterred from the conduct described above.

Other Outcomes: There are other tasks that a video surveillance system can be useful in accomplish which may from time to time prove valuable to the PSD such as diagnosis of false alarms and investigation of alleged employee misconduct, for example.

AUTHORIZATION

Video surveillance systems are authorized for use only in public places. In the event that misconduct on the part of a staff member is being investigated, no notification needs to be given prior to placing either covert or overt video surveillance tools.

Unless specifically authorized by the Superintendent in writing, all video surveillance system uses will be overt.

Covert video surveillance uses shall be undertaken only when individually authorized, in advance, by the Superintendent. Such uses shall be coordinated with law enforcement. Any such operation shall be narrowly focused, of limited duration, and will be dismantled upon conclusion of the investigation.

Video surveillance system access is limited to authorized users. The Superintendent shall specifically determine who may be granted system access, for what reasons, and at what permission levels. System access shall be logged. Each authorized user is responsible for ensuring that unauthorized does not occur at any terminal that the user is controlling. Unauthorized access includes allowing a person who have not received authorization to access or view the system, or allowing an authorized user to operate the system at a higher permission level than authorized. Unauthorized viewing includes allowing non-users to observe images when there is no legitimate reason for this observation. Copies of video shall not be provided to anyone, including parents and/or government officials unless legally compelled. Authorized users may allow non-users to see selected images for demonstration or operational purposes consistent with the District's mission, provided that such viewing does not violate any rules of evidence of confidentiality defined elsewhere in this document.

PSD is interested in operation video surveillance systems that are both efficient and effective, which can be supported and maintained affordably, that can be kept technologically current, and that have features consistent with policy and these procedures. Therefore, any and all video surveillance acquisitions shall be facilitated by and through the Director of Technology.

USE OF VIDEO SURVEILLANCE SYSTEMS

Areas of Surveillance

Only public places will be covered by a video surveillance camera. Private places will not be covered. There may be "gray" areas in terms of the public's expectation of privacy, and there may be areas that are clearly public, but which PSD nonetheless chooses to place limits on in terms of surveillance. If a need arises to cover such an area, application shall be made to the Superintendent who shall consider the request, and if appropriate, obtain a legal analysis. Written permission will be obtained. On occasion, the status of an area may change due to the designated use of the area at any given time, for example a classroom that maybe used as a visiting student sleeping area. Classrooms with video surveillance will have signage to that effect. Any camera covering such an area will be programmed to turn off (or manually disabled) during off-limits time. Such split-coverage will be approved in advance by the Superintendent or designee.

Facility Responsibility

Video systems will only be accessed by users who are authorized specifically by the Superintendent. The Director of Technology will have primary oversight of video operations, and will keep the Superintendent informed of any issues with the system. The Director of Technology is responsible for the day-to-day operations and all maintenance of that facility's equipment. They will track system performance, replace batteries and cleaning lenses as necessary, reporting system problems, installing video surveillance notice signage, and determining the extent live monitoring will occur.

Monitors shall not be left on when an authorized user is not viewing images on the video surveillance system. Users accessing any system remotely will remain signed in only while actively using that system. Video saps a great deal of network capacity, so users must not allow their sessions to run on unnecessarily or indefinitely.

The primary responsibility for live monitoring of overt systems (if it occurs at all) rests with the person in charge of a facility's system. From time to time, overt systems may be accessed and monitored as needed by other authorized PSD users external to facility staff. Examples include the Director of Technology, law enforcement, maintenance and operations (for building maintenance reasons), authorized administrators (for oversight, training, or demonstration reasons).

Covert systems will be monitored only with specific approval of the Superintendent, for participation in an operation/investigation.

RETENTION and STORAGE

To the maximum extent permitted by the equipment, motion images will be maintained for a minimum of 14 days. If a digital video recorder hard drive is over-writing motion images before 14 days has expired, then the person in charge must adjust the frame rate and/or resolution so that the minimum storage requirement is met. If accomplishing this task results in unacceptable degradation of image quality, then the person in charge should explore system enhancement.

All Digital Video Recorders (DVRs) will be properly secured to preserve the integrity of the record and prevent vandalism to the equipment itself. This generally means DVRs will be located in a secure room (such as a keyed communications closet,) or in a specially designed, locking DVR cabinet/case. Employees will not advertise the location of the DVRs to students or the public.

Pupil transportation will only use digital technology. Digital equipment will conform to the digital technology retention requirements.

The foregoing paragraphs deal with the total recorded record. Various portions of that record may be copied as "video clips" to support investigations and other operational activities. The retention schedule for clips differs from that of the total record. Clips supporting criminal, student discipline, and personnel matters will be maintained as set forth in the Video Evidence section, below. There is no

specific retention/destruction requirement for clops made for other reasons, but such clips should be retained as long as needed to meet the purpose of the clip, i.e., training, demonstration, etc.

LEGAL RESPONSIBILITY

Visual electronic records, like paper and email, may be subject to discovery and open records laws. Retention schedules, and storage procedures are to be adhered to so that electronic records that are requested can be produced, or an explanation provided as to why production cannot occur, i.e., the electronic record was overwritten pursuant to the record retention schedule.

NOTICE and SIGNAGE

Wherever an overt system is installed or activated, notices to that effect will be displayed about the premises. The site principal is responsible for ensuring that the signage is installed and maintained. The signs shall be prominently displayed, and state that the site is under 24 hour surveillance. Notice is not required for covert use of surveillance systems.

VIDEO EVIDENCE

Video clips supporting a criminal investigation will be turned over to law enforcement. The PSD (or other enforcement agency) is responsible for the maintenance, production, and destruction of that evidence. If a PSD employee retains a copy of the clip (generally for purposes of court preparation), he/she will restrict viewing according to the direction of law enforcement and/or prosecutor.

Video clips supporting a student discipline matter may become a “student record” when maintained as part of the disciplinary file. All District policies and FERPA requirements for student records apply to these clips.

Parents will have a limited access to viewing video, and is restricted to student discipline incidents, and they must be able to identify their child only. Thus, digital “pixelating” may be required. If multiple students are involved in a disciplinary incident, several versions of the clip may be necessary. It is the responsibility of the person in charge of the facility’s video surveillance system to make arrangements for the necessary digital enhancements. The Director of Technology will be responsible for performing this pixilation as necessary as directed by the Superintendent. Parents may consent under FERPA to let other parents view an unedited clip identifying their child. The extent to which parents in a given case agree to do this determines the degree to which “pixelating” can be eliminated in that case. Any such consent shall be obtained in writing. The signed form(s) shall remain permanently attached to the disciplinary case record. The clips will be retained and/or destroyed along with the file per existing policy.

Evidentiary video clips will be backed up, if possible showing uninterrupted recording for a reasonable period of time “surrounding” the event in question permitting the viewer to view the event in context of pre- and post-event occurrences, if any.

SYSTEM MAINTENANCE

The Director of Technology is responsible for initial system installation, general system administration and oversight. The site Administrator is responsible for reporting damage and malfunctions to the Director of Technology.

VIOLATIONS

Violations of these procedures may result in loss of video surveillance system access, and appropriate disciplinary action, or both.

DEFINITIONS

For purposes of these regulations and procedures, the following definitions are utilized:

FERPA (Family Educational Rights and Privacy Act of 1974): Please see the information link on FERPA. All district policy and program comply with FERPA regulations, as required.

Video Surveillance: A system that records video and sometimes sound. These devices can record either to the video unit themselves, or to a remote storage unit. Footage generated by these system can usually be downloaded from the system for documentation or storage. Most of the video systems likely to be deployed by PSD are IP based systems that require users to know the device address and have login credentials to be able to access.

Public Places: Areas of schools or other PSD facilities where the public has no reasonable expectation of privacy. These areas include, but are not limited to, playgrounds, fields, parking lots, entrances/exits, hallways, gym, multipurpose rooms, cafeterias, theaters, classrooms, libraries, labs, music rooms, and schoolbuses.

Private Places: Areas of schools or other PSD facilities where the public has a reasonable expectation of privacy. These areas include, but are not limited to, restrooms, locker rooms, dressing rooms, and showers.

Overt: A video surveillance application or use that is publicly acknowledged through notice or posting and/or through the use of cameras that are identifiable as such and clearly visible to observant users of the premises.

Covert: A video surveillance application or use that is not publicly acknowledged and that may incorporate hidden cameras.

Criminal Matters: An allegation that, if proved, would amount to a crime under municipal, state, or federal law. These matters require that evidence be seized, handled, stored, and destroyed in accordance with rules established through law and law enforcement procedure.

Discipline Matter: An allegation that, if proved, would amount to misconduct in violation of District, school or classroom policies such that the PSD may take disciplinary action against one or more individuals. These matters may require that evidence be collected, handled, releases and/or withheld, in accordance with law, District policy and negotiated agreements.

Adopted:
DATED :