Board Policies
2346 Safety and Security Video Monitoring

This policy governs the implementation of video surveillance and electronic monitoring systems on college property. This policy will also address the use of portable video cameras for security purposes.

This policy does not apply to video recordings of college events (e.g. plays, music performances, athletic contests, graduation, Board meetings), video recordings used for instructional purposes and made with the consent of all parties being recorded, video recordings made of individual teachers for the purpose of improving classroom instruction, or surveillance (covert or otherwise) undertaken by law enforcement officers.

Definitions:

1. **Covert Surveillance** – surveillance conducted by means of hidden devices, without notice to the individuals being monitored.

2. **Personally Identifiable Information** – all information about a student other than directory information, defined in R.C. 3319.321(B) (1).

3. **Video Recording** – a videotape, CD, DVD, disk, hard drive, or other device used to store information(whether in printed format, on film, by digital/electronic means or otherwise) from a video surveillance/electronic monitoring system.

4. **Video Surveillance/Electronic Monitoring System** – a video, physical, or other mechanical or digital surveillance/electronic monitoring system or device that is permanently installed and enables continuous or periodic video recording, observing or monitoring of individuals on college premises. This includes an audio device, thermal imaging technology or any other component associated with recording the image of an individual.

5. **Portable Video Cameras** – portable video cameras that may be carried by an individual.

Placement of Video Surveillance/Electronic Monitoring Equipment

Video surveillance/electronic monitoring equipment may not be used inside a classroom, laboratory, or other area utilized as a classroom. Neither shall they be operated in areas where there is a reasonable expectation of privacy (e.g. restrooms, locker rooms, private offices, conference/meeting rooms, and/or staff lounges).

No sound is to be monitored or recorded in connection with the video surveillance/electronic monitoring system.

Security staff and administrators are authorized to carry and use portable audio and video cameras when responding to a specific incident.

Notice of Surveillance

Each area in which video surveillance/electronic monitoring system occurs shall have clearly written signs posted at conspicuous locations informing persons that the buildings and grounds may be under video surveillance. Signs shall be conspicuous enough in size so that a reasonable person would be able to view the contents of the sign and have reasonable and adequate warning that surveillance is, or may be, in operation. The signs must provide contact information for the person who is responsible for answering questions about the video surveillance/electronic monitory system.

Operation of Video Surveillance/Electronic Monitoring Equipment

1. Video surveillance/electronic monitoring equipment may be used to monitor and/or record behavior and activity of all persons on college property or grounds.

2. Real-time viewing shall be limited to security personnel, administration or other employees needed to resolve the incident. Under certain circumstances, Security may contact local law enforcement to view the District's real-time video surveillance/electronic monitoring feeds.

3. Circumstances warranting a review should be limited to instances where an incident is reported/observed or to investigate a potential crime or violation of Board Policy or the Student Code of Conduct.

4. If information is not viewed for law enforcement, college or public safety purpose—it should be routinely erased according to a standard schedule (i.e. they will be maintained for a period of thirty (30) calendar days). If information is viewed for law enforcement, college or public safety purposes, it must be retained for a minimum of one (1) year. Prior to its destruction, the Superintendent and/or College Counsel must be contacted for approval.

5. A periodic audit of random images from the video surveillance/electronic monitoring system shall be conducted to verify that the equipment is operating properly and has not been blocked, moved or altered and that the images captured by the system are not inclusive of areas prohibited by this guideline.

6. Only a designated employee or agent of the Board can install and operate video surveillance/electronic monitoring equipment.

Use of Video Recordings

Information obtained through video surveillance/electronic monitoring shall be used exclusively to enhance security for students, staff and visitors, and to assist in the detection and deterrence of criminal activity(theft/vandalism) and/or violations of Board policy or the Student Code of Conduct. Video recordings may be used by the Board/administration as evidence in any legal or disciplinary actions, and for inquiries and proceedings related to law enforcement.

Any remote monitoring system must protect the integrity of the video surveillance system and include a system utilizing passwords or other identifiers to gain access. Monitoring shall only be conducted by authorized security administrators and designees (e.g. police officials). Likewise, network connected systems must not be openly accessible on the Internet; rather, they must be operated behind the District's firewall and password protected. Misuse or abuse of the video surveillance/electronic monitoring system shall not be tolerated and will be addressed on a case-by-case basis.

Viewing of Recordings

Any student (or parent of a minor student), employee or member of the public that is recorded by a video surveillance/electronic monitoring system has a general right of access to review the video if it will not result in or constitute an unauthorized release of another student's personally identifiable information. Access to an individual's own personal information may depend upon whether any other confidential or privileged information can be reasonably severed. Confidential or private information can be reasonably severed from the recording for viewing purposes if the District is able, without undue hardship or expense, to utilize a copy of the recording and digitally "black out" or "blur" the images of the other individuals who appear on the video. The original recording may not be altered in any manner. If an employee or student is facing any disciplinary action,s/he may authorize his/her (union) representative or other advocate to also view the video recording.

An individual may be refused permission to review a video recording where to allow it would:

1. be an unreasonable invasion of a third party's personal privacy;

2. give rise to a concern for the safety of a third party;

3. constitute an unauthorized disclosure of student personally identifiable information under State and/or Federal law; or

4. interfere with or compromise a law enforcement investigation/matter.

Retention, Secure Storage, Access to and Disposal of Video Recordings

Video recordings, when not in use, shall be stored in a locked, fire resistant cabinet or room, in an area to which students and the public do not normally have access. The recordings must be clearly and properly labeled and entered into a storage log.

Logs must be maintained of all instances of access to, and use of, recorded material – the log must document the person accessing the recording, the date and time of access, and the purpose). Security may authorize the viewing of recorded images in the event of an ongoing law enforcement investigation, and incident involving property damage or loss or for other reasons deemed appropriate.

All video surveillance/electronic monitoring recording media shall be considered legal evidence and treated as confidential. Release of original video recordings to individuals or outside agencies may only occur pursuant to subpoena or court order.

Original video recordings shall never be edited or manipulated in any manner. When video recordings are requested by any law enforcement agency as part of an ongoing investigation, a duplicate may be provided for that purpose. The original media shall be protected from accidental overwrite or erasure during the duplicating process. Nothing in this paragraph prohibits the redaction of personally identifiable information from duplicated media when mandated by FERPA.

Video recordings may never be sold publicly, viewed or distributed in any other fashion except as provided for by this guideline, and consistent with State and Federal law.

Video surveillance/electronic monitoring recordings shall be retained, stored and destroyed, including storage log books in accordance with this guideline.

Video recordings, scheduled to be destroyed must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved (e.g. shredding, burning, and magnetically erasing the personal information).

Covert Surveillance

Covert surveillance may only be used in cash handling areas, cashiers, safes, cash machines, vending machines and cash counting areas or when directed by law enforcement.

Adopted: 5-4-10