BOARD OF TRUSTEES
CARSON CITY SCHOOL DISTRICT

REGULATION No. 820
OPERATIONS

SAFETY AND SECURITY SURVEILLANCE MONITORING

Purpose

The Board of Trustees (the "Board") has recognized that maintaining the safety and security of students, staff, visitors, and property is best implemented through a multifaceted approach. To the extent modern technology provides tools to maintain safety and security, the use of technology such as video surveillance cameras has been supported by the Board. Video surveillance has been authorized for use in and around schools, on District property, and on school transportation vehicles. Cameras may be equipped with audio recording capabilities as well. Audio and video surveillance ("video surveillance") shall be in accordance with applicable laws pertaining to such use. The District also shall comply with applicable law related to maintaining video recordings. This regulation governs the use of video surveillance in accordance with applicable law.

Scope

This regulation applies to all property that is under the ownership or control of the School District and regulates the actions of District personnel who are responsible for installing or operating video surveillance equipment and systems.

Approval, Installation, and Operation

1. Video and electronic surveillance systems shall only be installed and operated following prior review and approval by the Risk Manager or his/her designee and only as outlined in this regulation. Cameras equipped with audio recording capabilities are also subject to prior review and approval by the Risk Manager or designee.

2. Exceptions to the prior review and approval requirement may be made in the event of an emergency or an imminent threat to the safety and security of the school community, and only as outlined in this regulation.

3. Video surveillance systems shall be installed, administered, and managed centrally through the I.T. Department. The video surveillance equipment will be inventoried and maintained as a District asset.

4. Video surveillance systems shall be installed and operated by a limited number of authorized operators who:

a) demonstrate a legitimate need for such access consistent with the purposes of this policy;
b) are appropriately trained and supervised in the responsible use of these systems, and
c) are approved in writing by the Risk Manager or designee.

5. Video surveillance monitoring systems will not be monitored in real time on a 24 hour / 7 day basis.

Appropriate and Prohibited Uses

1. Video and electronic surveillance systems shall not be installed in or used to monitor or record areas where there is a reasonable expectation of privacy in accordance with accepted social norms. These areas include but are not limited to restrooms, locker rooms, changing or dressing areas, health treatment rooms, and counseling offices.

2. Video surveillance systems shall not be used to monitor or record sensitive institutional or personal information which may be found, for example, on an individual's workspace, on a computer or other electronic display.

3. Surveillance information obtained through video and electronic surveillance systems shall not be accessed, used, or disclosed except as outlined in this regulation.

4. Operators are prohibited from:
    a. Monitoring individuals based on inappropriate characteristics such as race, gender, ethnicity, sexual orientation, or disability;
    b. Duplicating images or permitting access to others of surveillance images except as specifically permitted by this policy; and
    c. Viewing, recording, accessing, or otherwise using a surveillance system or surveillance images in any manner that is inconsistent with this regulation and/or outside the scope of the access approved by the designated campus authority in accordance with this regulation.

Notification

1. Public notice of the video surveillance, in the form of signage, will be displayed at all video surveillance locations, except at emergency or investigative locations.

Monitoring and Recording Evidence

1. Any information collected through the use of video surveillance equipment is considered District property and/or records. The Principal or designee at each school will be responsible for determining the specific personnel who will have access to video surveillance equipment and recordings.

2. Upon notification of potential criminal or unauthorized activity in a particular location, Safety Services personnel may review information obtained from the video surveillance equipment in conjunction with its investigation of such activity.

3. The Safety Services Department may conduct or monitor video surveillance upon any area that is open and accessible to the District in accordance with state and federal privacy laws.

4. This regulation does not apply to surveillance utilized by law enforcement agencies for criminal surveillance as permitted by law.

5. The District will take reasonable security precautions to prevent unauthorized access to, use, or disclosure of data recorded by video surveillance systems.

Investigations

2. Investigations conducted by Safety Services, school administration, School Resource Officers or the Transportation Director may involve a review of video and/or bus surveillance recordings. These recordings are the property of the District and there is no obligation by the District to allow access to, or viewing of, those recordings by individuals, unless otherwise required by law.

3. Principals (for school video) and supervisors approved by the Transportation Director (for bus video) may, at their discretion, allow the viewing of recorded video by individuals not employed by the District for the purpose of handling routine disciplinary issues. In those instances, primary consideration should be given to protecting the privacy of others depicted in the video and the identity of potential witnesses.

4. Pursuant to the terms of the District's Memorandum of Understanding with the Carson City Sheriff's Department, the Sheriff's Department shall have access to the District's video surveillance system for use in civil and criminal investigations.

Requests for Access by Third Parties or Entities

1. Requests for access to video surveillance recordings received by the District from persons or entities (including current or former District employees) shall be immediately forwarded to the Risk Manager. Upon receipt of a request for access, whether in the form of a request under the Family Education Rights and Privacy Act ("FERPA"), civil or criminal subpoena, search warrant, a Nevada Public Records Act request, a request of a current or former employee pursuant to Labor Code, Court Order, or other form, immediate steps shall be taken to preserve the recording, until access rights are determined.

2. Video surveillance recordings generally are not subject to public inspection. However, because the District may be required by law to respond to requests for access, the District's Risk Manager and General Counsel will be consulted to assist with responding to requests for access by parents and members of the public. If, after such consultation, the District authorizes access to or release of a copy of a recording, the District will ensure that the original of the recording is retained in the District's files.

3. Requests for video surveillance recordings that involve or are related to potential employee misconduct, including those requested by current or former employees or law enforcement, will be forwarded to the District's Human Resource Department for review. A recording or image of a staff member that may be used in a personnel action is subject to the laws and regulations regarding school personnel actions, including an employee's right to comment on derogatory information placed in his or her file.

REGULATION No. 820 - CONTINUED

Collection, Storage, and Disposal of Information

1. Video surveillance recordings may not be altered in any respect. Surveillance equipment centers and monitors will be configured to prevent operators from tampering with or duplicating recorded information.

2. No third-party software shall be used to extract, capture, export, or otherwise manipulate files originating from the District video surveillance system software or servers.

3. Surveillance records shall not be stored on individual computer hard drives, portable storage devices such as "flash drives", "thumb drives", or mobile cellular devices. All surveillance records shall be stored on a secure server location for a period of 21 days and will then promptly be erased or written over, unless retained as part of a criminal investigation or court proceedings (criminal or civil), or other bona fide use as approved by the Risk Manager.

4. Recordings from surveillance equipment may be preserved and retained longer than 21 days under specific circumstances. This retention may occur:
   a. Upon receiving credible notification of a District or law enforcement investigation for alleged illegal activity or violation of district policy or school rules.
   b. Upon receiving notice from the office of General Counsel that such copying and storage is otherwise needed to comply with legal obligations to retain materials;
   c. Where there is a reasonable belief that the surveillance information may be related to illegal activity that has occurred, is occurring or is imminently about to occur; or
   d. Where the surveillance information has historical significance.

   Video surveillance recordings must be destroyed in a secure manner as soon as they are no longer needed.

Training

1. Operators shall be provided a copy of the District's policy, this regulation, the related system operating guidelines for appropriate use, and an Acceptable Use Agreement, by which they must acknowledge in writing that they have read, understood, and agree to the contents thereof. Such documents and agreement prohibit the targeting of individuals based upon perceived individual characteristics or classifications such as race, gender, ethnicity, sexual orientation, or disability.

2. Surveillance equipment operators will:
   a. Receive training on technical, legal and ethical use of such equipment;
   b. Provide written acknowledgement that they have read and understand this policy;
   c. Perform their duties in accordance with this policy; and
   d. Access images only to the extent permitted by this policy.

Compliance with Laws

The Risk Manager, or designee, in consultation with in the District's General Counsel, will monitor new developments in the relevant law and in security industry practices to ensure that the manner in

which the District utilizes video surveillance is consistent and compliant with the highest standards and protections, and any applicable laws.

Violations and Sanctions

Violations of any aspect of this regulation may subject the violator to employment, civil or criminal action, as permitted by District policy, applicable collective bargaining agreement(s), and/or any applicable laws.

Implementation Guidelines & Associated Documents

This policy aligns with the following CCSD governing documents:
Regulation 218, Internet Safety and Network Acceptable Use
Regulation 515 and 515.3 Student Education Records
Safety Services Bulletin: Surveillance System Operating Guidelines

Reference: NRS 200.650

Adopted: February 13, 2018