Emery County School District

Policy: ECAF—Video Surveillance

Date Adopted: 6 May 2015
Current Review / Revision: 6 May 2015

For the safety and security of the buildings, assets, staff and visitors, the Emery County School District operates a video-surveillance system in our schools and randomly on school buses. This video surveillance policy describes the District's video surveillance system and the safeguards that the District implements to protect the personal data, privacy and other fundamental rights and legitimate interests of those recorded on the cameras.

Purpose

The Emery County School District uses its video surveillance system for the purposes of security, access control and monitoring behavior in school buildings, as well as on buses and school property. The video surveillance system helps insure the safety of our staff, students and visitors, as well as property and information located or stored on the premises. It complements other physical security systems such as access control systems and physical intrusion control systems. It forms part of the measures to support our broader security policies and to help prevent, deter, and if necessary, investigate unauthorized physical access, as well as disruptive or illegal behavior. In addition, video surveillance helps prevent, detect and investigate theft of equipment or assets owned by the District, visitors, students or staff, and threats to their safety.

Purpose Limitation

The system is not used to monitor the work of employees or to monitor attendance. Neither is the system used as an investigative tool (other than investigation related to physical security, personal safety incidents, such as thefts or unauthorized access, and to reasonably detect inappropriate actions and/or illegal behavior of individuals on school property.

Surveillance Equipment Used

The video surveillance system, used in school facilities, is a conventional static system. It records digital images and is equipped with motion detection. It records any movement detected by the cameras in the area under surveillance, together with time, date and location. All cameras operate 24 hours a day, seven days a week. The image quality in most cases allows identification of those in the camera's area of coverage

The cameras are all fixed (there are no pan-tilt-and-zoom cameras), and thus, they cannot be used by the operators to zoom in on a target or follow individuals around. We do not use high-tech or intelligent video surveillance technology and we do not interconnect our system with other systems. We do not use covert surveillance, sound recording, or "talking CCTV"

Areas Under Surveillance

Cameras may be located at entry and exit points of our buildings, including the main entrance, emergency and fire exits and the entrances to the parking lots. In addition, there may also be a camera at the entrance to the stairways, public

hallways, outside grounds and event areas. Cameras are also randomly placed on school buses. Bus surveillance is under the direction and supervision of the Transportation Supervisor.

Areas of Heightened Expectations

Video surveillance is not used to monitor any areas under heightened expectations of privacy such as individual offices, classrooms, labs, staff leisure areas, toilet facilities and sports locker rooms.

Video System Modifications and Expansion

The current video surveillance system may not be modified, expanded, relocated or otherwise altered without direct and prior consultation with the District Technology Supervisor.

Notification of Video Surveillance

Each District site that implements video surveillance must provide notification to the public that video is being recorded on the premises (i.e. a sign posted on the front door of a school).

Access to Video Surveillance Information

Recorded video is accessible to school and district administrative staff only and to a designee of the building administrator. Live video is also accessible to administrators and the designee.

The District's administrators and designee have the right to:

- View the footage real-time,
- View the recorded footage, or
- Copy,
- Download,
- Delete, or
- Alter any footage.

Periodic System and Video Image Audit

A periodic audit of the surveillance system and video images shall be conducted by the District Technology Supervisor to ensure the surveillance system has not been modified or altered and to ensure the integrity of the system.

System Monitoring and Security

Due to activities of the administrative staff video may not be monitored continuously. Devices used to view live and recorded video will have secure access and be located out of open view of the public and staff. Visitors students and staff should be aware that an administrator is not watching most cameras most of the time and they should not have an expectation that they are under continuous surveillance when they are in the range of a camera.

Data Protection Training

All personnel with access rights will be provided video and data protection training and periodic workshops on video and data protection compliance issues are carried out at least once every two years for all staff with access rights.

Confidentiality Undertakings

After being trained, each staff member with access to video surveillance, must sign a confidentiality agreement.

Transfers and Disclosures

All transfers of video content and disclosures outside administration are documented and are subject to a rigorous assessment of the necessity of such transfer and the compatibility of the purposes of the transfer with the initial security and access control purpose of the processing. In most cases, the transfer of video content is limited to judicial subpoenas or if requested by the school/district administrator.

Local police may be given access, by the building administrator or the District Supervisor of Technology, if needed, to investigate or prosecute criminal offenses.

Data Retention

The images or video content are retained for a maximum of 14 days. Thereafter, all images may be deleted or overwritten. If any image/video content needs to be stored for further investigation or evidence in a security incident, it may be retained as necessary.