[District] Video Surveillance Policy Template

1. Purpose and scope of the District's video surveillance policy
For the safety and security of its buildings, assets, staff and visitors, our District operates a video surveillance system. This video surveillance policy describes the Districts video surveillance system and the safeguards that the District takes to protect the personal data, privacy and other fundamental rights and legitimate interests of those caught on the cameras.

2. Purpose of the surveillance
The District uses its video surveillance system primarily for the purposes of security and access control. The video surveillance system helps control access to our building and can helps ensure the security of our building, 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 supports our broader security policies and helps prevent, deter, and if necessary, investigate unauthorized physical access. This includes unauthorized access to secure premises and protected rooms, IT infrastructure, or operational information. 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.

3. What areas are under surveillance

3.1. Type of equipment in use
The video surveillance system 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 areas 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"

3.2. Video system modifications and expansion
The current video surveillance system will not be modified or expanded. Equipment will not be moved modified or relocated or otherwise altered without direct and prior consultation with the designated district administrator. All additions or modifications must be approved in writing with a signature of the district superintendent or designee.

3.3 Camera locations and coverage
Cameras are 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 is also a camera at the entrance to the stairways, public hallways, outside grounds and event areas.

3.4 Areas of heightened expectations
We specifically do not allow monitoring any areas with heightened expectations of privacy such as individual offices, classrooms, labs, staff leisure areas, toilet facilities and sports locker rooms.

3.5 Notification of video surveillance
A district site that implements video surveillance must provide written notification, (i.e. a sign posted on the front door at school to the public that video is being recorded on the premises).

4. Who has access to the information and to whom is it disclosed

4.1. School Administrators and Designee of the District Superintendent
Recorded video is accessible to a designee, school and district administrator only. Live video is also accessible to administrators and designee. Recording may be suspended without prior acknowledgement of students, staff, and district administrators.

4.2. Periodic system and video image audit
A periodic audit of the surveillance system and video images shall be conducted by the superintendent or designee to verify the surveillance system has not been modified or altered and to improve the integrity of the system.

4.3 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.

4.4. Access rights
The district's administrators and designee may:

View the footage real-time
View the recorded footage

The district will maintain a list of district employees with video access authority.

4.5. Data protection training
All personnel with access rights will be provided video and data protection training. Training is provided for each new member of the staff and periodic workshops on video and data protection compliance issues are provided on regular basis for all staff with

access rights.

4.6. Confidentiality undertakings
After the training each staff member will sign a confidentiality agreement. Violation of the agreement may have employment and or professional consequences.

4.7. Transfers and disclosures
All transfers of video content and disclosures beyond district administration should be documented. Such transfers shall be limited to judicial subpoenas.
Local police may be given access to video by subpoena or if requested by the school/district administrator.

5. How long do we keep the data
The images or video content are retained for a maximum of ___ days. Thereafter, all images are 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.