EDMONTON PUBLIC SCHOOLS

Administrative Regulation

CODE: DCA.AR

TOPIC: Video Surveillance Systems

EFFECTIVE DATE: (29-01-2020)

ISSUE DATE: (29-01-2020)

REVIEW YEAR: (2025)

OBJECTIVE

- To ensure the legal and ethical use of video surveillance systems used to maintain a safe and secure environment in Division schools and facilities.
- To ensure that the Division achieves balance between the benefits of video surveillance systems and the privacy of the individual.
- To provide clarity and consistency in processes to install, use and maintain video surveillance systems and manage the personal information recorded by video surveillance systems.

DEFINITIONS

Digital Video Recorder is an electronic device that records video in digital format to a storage device.

Division school or facility means a school operated by Edmonton Public Schools or a facility that is owned or operated by Edmonton Public Schools.

Extracted recording is a recording created by making a digital copy of a video recording from a video surveillance system.

Law enforcement refers to all of the following:

- policing, including criminal intelligence operations
- a police, security or administrative investigation, including the complaint giving rise to the investigation, that leads or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred
- proceedings that lead or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the proceedings or by another body to which the results of the proceedings are referred

Real time video surveillance is where a video surveillance system is monitored in real time.

Personal information is defined under the *Freedom of Information and Protection of Privacy Act (FOIP Act)*. Personal information means recorded information about an identifiable individual.

System log refers to a record created by the video surveillance system software which documents the username, the date, time and the activity of the user.

Video surveillance occurs when a record of images is created and retained by recording activity in an area or building using a secured camera system or when live-stream images from a secured camera system are monitored in real time.

Video surveillance does *not* include:

- instances where school officials video record or live stream a specific event (such as a school play, concert, sporting event or graduation ceremony)
- an isolated incident where a classroom is video recorded for educational or research purposes

Video surveillance system is the hardware and software components required to capture and store video recordings on an ongoing basis including a camera, a digital video recorder, a method to securely transfer the images from the camera to the digital video recorder and software to manage the processes.

Video surveillance system software is the software used to access, view and extract the video recordings created by the video surveillance system.

RESPONSIBILITY

1. Only a principal or a Decision Unit (DU) administrator responsible for a Division school or facility may request the installation, expansion or replacement of a video surveillance system.

2. Security Services shall collaborate with principals and DU administrators to complete the request for video surveillance systems including the specific details regarding camera placement and the Privacy Impact Assessment.

3. Infrastructure shall ensure that if video surveillance cameras are used to record video on buses, the requirements of this regulation shall be included as terms and conditions of any service contract with the service provider.

4. The Video Surveillance Systems Review Committee, comprised of the Division FOIP Coordinator or designate and representatives from Security Services and District Support Services, has the responsibility to review and approve or reject applications for video surveillance systems based on the requirements of this regulation.

5. In the event of the rejection of an application for a video surveillance system, a principal or DU administrator may appeal the decision to a committee composed of the General Counsel, the Assistant Superintendent of Infrastructure and the Assistant Superintendent of their school or DU, which will make the final determination.

6. The principal or the DU administrator responsible for a Division school or facility may not engage in real time viewing of video surveillance systems or delegate real time viewing of video surveillance systems unless it is for a specific law enforcement purpose, or for monitoring the school or facility during a lockdown procedure, or for monitoring locked entry doors to control access to a Division school or facility.

7. Notwithstanding any other provision in this regulation, the Superintendent may authorize the installation, expansion, replacement or removal of a video surveillance system on behalf of the Division.

REGULATION

A. RATIONALE REQUIRED TO REQUEST VIDEO SURVEILLANCE SYSTEMS

1. In accordance with the *Freedom of Information and Protection of Privacy Act* (*FOIP Act*), the Division may only use personal information collected by a video surveillance system to support the safety of staff and students and the security of Division schools and facilities. This includes use in an investigation that could possibly lead to disciplinary (both student and staff), legal, legislative or law enforcement purposes; enforcement of Division administrative regulations; or for a consistent purpose; or in accordance with a court order.

   Video surveillance systems may only be used where conventional measures for achieving law enforcement or public safety objectives, such as increased staff supervision or security guard patrol are substantially less effective or are not feasible, and the benefits of video surveillance substantially outweigh the reduction of privacy inherent in collecting personal information using a video surveillance system.

2. To request approval for the installation, replacement or expansion of a video surveillance system, a principal or DU administrator, working with Security Services, shall submit a written rationale to the Video Surveillance Review Committee including but not limited to:
   a. the completion of the Privacy Impact Assessment in consultation with Security Services and the Division FOIP Coordinator
   b. verifiable, specific reports of incidents of crime, vandalism or safety and security concerns
   c. examples of other measures of deterrence or detection that have been used or considered, and the reasons why those measures are less effective or not effective for the concern being addressed
   d. results of consultation with stakeholders including students, parents and staff regarding the necessity of the proposed video surveillance system in the school or facility
   e. the identification of the location(s) of the proposed video surveillance camera(s) to provide viable measures of deterrence or detection
   f. plans for the design and operation of the proposed video surveillance system that minimize intrusion on personal privacy.

B. INSTALLATION OF VIDEO SURVEILLANCE SYSTEMS

1. Any video surveillance system connecting to the Division's network must meet the Division's information technology standards.

2. Video surveillance cameras must not be directed towards property or windows of property adjacent to Division schools or facilities.

3. Video surveillance cameras must not be used to monitor areas where individuals have a reasonable expectation of privacy including, but not limited to, change rooms and washrooms.

C. NOTIFICATION REQUIREMENTS FOR THE USE OF VIDEO SURVEILLANCE SYSTEMS

1. If a video surveillance system is installed or used in a Division school, the principal must notify students, parents and school staff of the following points at the beginning of every school year:
    a. the video surveillance system is to assist in maintaining a safe and secure environment
    b. the video surveillance system will be used to record and may be used to monitor activity
    c. personal information collected by the video surveillance system may be used and/or disclosed in an investigation that could possibly lead to disciplinary (both student and staff), legal, legislative or law enforcement purposes, for enforcement of Division administrative regulations, or for a consistent purpose, or in accordance with a court order.

2. If a video surveillance system is installed or used in a Division facility, the DU administrator responsible for that Division facility must notify Division staff at that facility at least yearly that:
    a. the video surveillance system is to assist in maintaining a safe and secure environment
    b. the video surveillance system will be used to record and may be used to monitor activity
    c. personal information collected by the video surveillance system may be used and/or disclosed in an investigation that could possibly lead to disciplinary (both student and staff), legal, legislative or law enforcement purposes, for enforcement of Division administrative regulations, or for a consistent purpose, or in accordance with a court order.

3. If a video surveillance system is used in a Division school or facility, the principal or the DU administrator must ensure that the approved signs attached to this regulation are prominently posted at each entrance to the Division school or facility under video surveillance notifying people that the Division school or facility is under video surveillance. If there are video surveillance cameras monitoring the outside of the building, signage must also be displayed outside the main entrance of the building.

D. MAINTENANCE OF VIDEO SURVEILLANCE SYSTEMS

1. A prescribed maintenance program shall be established by the Division, and all sites with video surveillance shall adhere to the prescribed schedule.

E. AUTHORIZED ACCESS TO VIDEO SURVEILLANCE SYSTEMS

1. If a video surveillance system is in use in a Division school or facility, the principal or DU administrator must ensure that all of the following conditions are in place:
    a. Physical access to the digital video recorder is restricted to the principal, DU administrator, Security Services staff, Infrastructure Maintenance Staff, General Counsel or the Division FOIP Coordinator for the performance of their duties.
    b. The principal or DU administrator shall audit and monitor who is accessing the video surveillance system software and its recordings through the use of the system log.

2. The video surveillance system recordings may only be reviewed by the principal or DU administrator when a specific incident or event occurs that requires an investigation. Some examples of the circumstances that would merit a review of video surveillance recordings include, but are not limited to:
    a. incidents of safety and security that have been reported or observed
    b. for disciplinary, legal or legislative purposes
    c. for a law enforcement matter.

3. Division employees may review video surveillance system recordings through the video surveillance system software when they are required and authorized to do so by the principal or DU administrator in the performance of their duties, but only to the minimal extent necessary to fulfill their duties.

4. School Resource Officers (SROs) may review video surveillance system recordings through the video surveillance system software in accordance with the Information Sharing Agreement with the Division.

F. RETENTION AND SYSTEM LOGS OF VIDEO RECORDINGS

1. A system log shall be created when an extracted recording is made for any purpose. The information in the system log may be required by the Division FOIP Coordinator, Security Services, or General Counsel. The system log, extracted recordings and recordings stored on the digital video recorder shall be retained in accordance with the Division's records retention schedule.

G. ACCESS REQUESTS FROM LAW ENFORCEMENT

1. Any request from law enforcement to view or for release of a video surveillance system recording, video recording device or an extracted recording from a Division school or facility must be referred to the principal or DU administrator who must ensure that the Law Enforcement Disclosure Form is completed before the video surveillance system recording, video recording device or the extracted recording is viewed or released.

H. RIGHT OF ACCESS UNDER THE *FOIP ACT*

1. An individual whose personal information has been collected and recorded by a video surveillance system may request access to their own personal information in accordance with the *FOIP Act*.

2. Any individual may request access to a video surveillance system recording or an extracted recording in accordance with the *FOIP Act.*

I. REAL TIME MONITORING OF VIDEO SURVEILLANCE SYSTEM

1. Real time video surveillance may be used to monitor locked entry doors of Division schools and facilities. Only employees appointed by the principal or the DU administrator responsible for the Division school or facility will monitor, in real time, entry cameras in order to respond to requests to enter the Division school or facility.

2. Where feasible, all Division elementary schools, elementary/junior high schools and junior high schools shall have installed real time video surveillance to control access to the school building.

3. In the event of a lock down procedure, the principal or DU administrator, or their designate, Division Security and the SRO may have real time video surveillance access to the video surveillance system. Such access to real time video surveillance through the video surveillance system software shall be secured by username and password and shall only be used during a lock down procedure.

J. EXCLUSIONS

1. This Administrative Regulation does not apply to surveillance cameras used for law enforcement purposes as a case-specific investigation tool where there is legislative authority or a court order authorizing the surveillance.

REFERENCES

CN.AR - Creation, Use and Maintenance of Division Information
CW.AR - Purchasing and Disposal
DCA.BP - Security and Vandalism
DK.BP - Division Technology
DK.AR - Division Technology Standards
Division Records Retention Schedule
Freedom of Information and Protection of Privacy Act
Law Enforcement Disclosure Form