



Northeastern Catholic District School Board

VIDEO SURVEILLANCE

Administrative Procedure Number: API004

POLICY STATEMENT

The NCDSB takes the responsibility of student and staff safety very seriously. To that end, and in compliance with its responsibility and duty of its employees as per the *Education Act*, video surveillance equipment will be utilized. Video surveillance and the resulting records are to be used for inquiries and proceedings related to maintaining the health, welfare, safety and security, for the protection of property and any criminal activity-affecting students, staff, and visitors while on school board premises.

REFERENCES

Education Act

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

Guidelines for the Use of Video Surveillance, 2015 (Information and Privacy Commissioner of Ontario)

NCDSB Policy E-30 Joint Transportation

NCDSB Policy E-34 Safe Schools

NCDSB Policy I-2 Responsible Use of Information Communication & Technology

NCDSB Policy P-4 Personal Information Management

NCDSB Procedure APP025 Breach of Personal Information

DEFINITIONS

Board Property includes school buildings, grounds, and facilities under the jurisdiction of the Board.

Video surveillance equipment refers to video, physical or other mechanical, electronic, or digital surveillance system or device that enables continuous or periodic video recording, observing, monitoring or individuals in school buildings and on school premises.

Storage device and recorded media refers to a videotape, computer disk or drive, CD-ROM, computer chip, or other devices used to store the recorded data or visual, audio, or other images captured by a video surveillance system.

Reception equipment refers to the equipment or device used to receive or record the personal information collected through a video surveillance system, including a camera or video monitor or any other video, audio, physical or other mechanical, electronic or digital device.

Personal information is defined as being recorded information about an identifiable individual, which includes, but is not limited to , information related to an individual's race, colour, national or ethnic origin, sex and age.

Covert surveillance is defined as the secret, continuous or periodic observations of persons, vehicles, places, or objects to obtain information concerning the activities of individuals which is then recorded in material form

PROCEDURES

1.1. Authorization to use Surveillance Equipment

- 1.1.1. The Principal and/or designate is responsible for the proper implementation and control of the video surveillance program in a school.
- 1.1.2. Video surveillance equipment will only be adopted where circumstances have shown that it is necessary for the purpose of enhancing safety or for the deterrence of destructive acts, such as vandalism. Before implementing a video surveillance program, a school or facility should be able to demonstrate:
 - a. a history of incidents (e.g., intrusion, personal safety issues) occurring in the specific school / facility;
 - b. the effect of the physical circumstances of the school/facility – does it permit ready access to unauthorized individuals; and
 - c. whether a video security surveillance program would be effective in dealing with or preventing future incidents of the type that have already occurred.
- 1.1.3. The Principal will conduct an assessment, including input from students, staff, and the Catholic school council, into the effects that the surveillance system will have on personal privacy in the school and the ways in which such adverse affects may be mitigated.
- 1.1.4. A report will be provided by the Principal to the appropriate Superintendent describing the circumstances that indicate the necessity of having surveillance at that site, including a review of less invasive alternatives.
- 1.1.5. Video surveillance equipment locations will be authorized by a Superintendent, upon the recommendations of the Principal and the Manager of Plant and Facilities, and the Manager of Information Communication & Technology. Any change in camera location must be authorized in the same manner. Video surveillance equipment shall not monitor the inside of areas where students, staff, and the public have a higher expectation of privacy (e.g., change rooms and washrooms). Video surveillance will only be used in other areas where the public has a higher expectation of privacy such as meeting rooms or offices, with the approval of the Director of Education and/or designate.
- 1.1.6. Public notification signs clearly written and prominently displayed, notifying individuals of the recording and school office contact information for any questions, must be in place in areas that are subject to video surveillance.

- 1.1.7. Remote access will only be used by the Manager of Information Communication & Technology and/or designate, the Manager of Plant and Facilities and/or designate to assist and support investigation of serious incidents and to maintain the deployed systems.
- 1.1.8. The Superintendent of Business and/or designate will be responsible to ensure that service providers are aware of and comply with this procedure when video surveillance is required on school vehicles.

1.2. Installation of Video Surveillance Equipment

- 1.2.1. Video surveillance equipment will be installed only by a designated employee or third party service provider of the Board.
- 1.2.2. Video monitors will not be located in an area that allows for public viewing.
- 1.2.3. Video surveillance equipment will be installed in a way that it only monitors areas that have been identified as requiring video surveillance. Cameras will not be directed to look through the windows of adjacent buildings or onto adjacent property. Cameras will be operated continuously.
- 1.2.4. If the video surveillance equipment is adjustable by the operators, this practice will be restricted so that the operators will not be able to adjust or manipulate the equipment to overlook areas not intended to be covered.
- 1.2.5. Maintenance of the cameras and the video surveillance equipment is the responsibility of the Information Communication & Technology with support from the Plant and Facilities Department and the third party service provider of the Board.
- 1.2.6. The annual preventative maintenance program for recorders and cameras will include refocusing and lens cleaning while ensuring that the equipment is operating properly and in accordance with the manufacturer's specifications. Any issues or concerns regarding the performance of such equipment will be followed up promptly by the Information Communication & Technology department. Email techsupport@ncdsb.on.ca for any incidents associated to video surveillance systems and cameras.
- 1.2.7. The installation of video surveillance equipment by third party service providers operating in our schools / facilities (tenants on Board property) must follow this procedure.
- 1.2.8. The installation of fake or dummy cameras is prohibited.
- 1.2.9. Any agreements between the Board and the third party service providers will state that the records dealt with or created while delivering video surveillance services will be subject to the Board's policy, administrative procedures, and the *Acts*.

1.3. Viewing of the Storage Device

- 1.3.1. Any designated person who accesses and/or uses a storage device will be responsible to complete the appropriate form electronically, which will be submitted to the Privacy Information Management Officer of the Board.
- 1.3.2. The storage device will be viewed only by a Principal, a Superintendent, the Director of Education, the Manager of Information Communication & Technology, the Manager of Plant and Facilities, the Police Services, by parents, and students (subject to 1.3.5. below), or other staff with a direct involvement with the recorded contents of the specific storage device, or employees of third party service providers responsible for the technical operations of the system (for technical purposes only).
- 1.3.3. Search and review capabilities on digital systems must be protected by password access.
- 1.3.4. The student shall be allowed to view at his/her request, any of the student's personal information which has been recorded and retained by the Board subject only to exemptions under the Act. Special attention should be given to students that have reached the age of majority when considering requests to view a student's personal information that has been recorded and retained by the Board.
- 1.3.5. Student or parent/guardian viewing must be done in the presence of the Principal and/or their designate. Consider 1.3.4 when considering the request.
- 1.3.6. Viewing may be refused or limited where viewing would be an unreasonable invasion of a third party's personal privacy, would give rise to a third party's safety, or on any other grounds recognized in the *Municipal Freedom of Information and Protection of Privacy Act*.

1.4. Handling of the Storage Device and Recorded Media

- 1.4.1. The Storage device and recorded media will be stored in a secure room in a controlled access area.
- 1.4.2. Each storage device will be dated and labeled with a sequential number. A log will be kept of all instances of access to, and use of recorded material to enable a proper audit trail.
- 1.4.3. The storage device and recorded media may never be sold, publicly viewed or distributed in any other fashion except as provided for by Policy (Policy F-27) and appropriate legislation.
- 1.4.4. The storage device and recorded media will be erased within three months unless they are being retained at the request of the Board or are being transferred to the Board's insurers or the Police Services. Digital systems shall be configured so that they archive for a maximum of three months.
- 1.4.5. Access by an employee, parent, or student for documentation related to a specific incident may be granted at the discretion of the Director of Education.

- 1.4.6. Where recorded information has been used for a law enforcement, school or public safety purpose, the retention period shall be one year after it has been last used, and/or all appeals relating to a particular incident have been exhausted.
- 1.4.7. Old storage devices will be disposed of in such a way (i.e., shredding, burning or magnetically erasing) that the personal information cannot be reconstructed or retrieved. The Information and Communication Technology Department will be responsible for the disposal of video surveillance equipment, including storage devices. The disposal of the record shall be noted in the log.

1.5. Governance

- 1.5.1. The Principal and/or their designate are responsible for the proper implementation and control of the video surveillance program in the schools. The Information and Communication Technology Department and the Plant and Facilities Department will provide support and will assist with the implementation and control of video surveillance programs to maintain established standards and infrastructure. The Superintendent of Business and/or designate will be responsible to ensure that School Bus Operators that are using surveillance equipment in their vehicles are aware of this procedure.
- 1.5.2. The Director of Education will facilitate regular reviews of these procedures in consultation with appropriate school and system staff. Changes will be communicated in a timely manner to all those impacted.
- 1.5.3. The Director of Education will facilitate a review of the “installed” video surveillance equipment at least every three years, in consultation with the appropriate managers, superintendents, and principals.

1.6. Misuse and Consequences of Misuse

- 1.6.1. Video monitoring must be carried out in accordance with these procedures.
- 1.6.2. The improper use of video surveillance will not be tolerated and will result in appropriate administrative or disciplinary action in any cases of wrongful use.
- 1.6.3. In the event of a breach of privacy the school principal will:
 - a. Identify the scope of the potential breach and take steps to contain it;
 - b. Identify those individuals whose privacy was breached and, barring exceptional circumstances, notify these individuals accordingly;
 - c. Notify the Director of Education and the Privacy Information Management Officer of the Board.

1.7. Covert Surveillance

- 1.7.1. Prior to the use of covert surveillance a case must be presented by the Principal and/or the Department Manager to the Director of Education for approval on the grounds that covert surveillance is essential to the success of a possible criminal investigation and the need outweighs the privacy of the persons likely to be observed.

1.7.2. The case and supporting documentation must identify the benefits which will be derived from the investigation.

1.7.3. The covert surveillance must be time limited and case specific.

1.8 Related Forms

Electronic Template – Access to Video Surveillance Storage Device and Recorded Media

Director of Education: *Tricia Stefanic Weltz*

Date: **November 2019**