Northeastern Catholic District School Board

VIDEO SURVEILLANCE

Administrative Procedure Number: API001

POLICY STATEMENT

The Northeastern Catholic District School Board (NCDSB) is committed to maintaining safe, secure, and respectful learning environments for all students, staff, and visitors. To support this commitment, and in accordance with the *Education Act* and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), video surveillance may be used on Board property.

Video surveillance systems shall be implemented and operated in a manner that respects individual privacy rights, is consistent with our Catholic values, and is limited to purposes such as enhancing safety, protecting property, deterring criminal activity, and supporting investigations of serious incidents.

REFERENCES

Education Act
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
Information and Privacy Commission of Ontario, 2015: *Guidelines for the Use of Video Surveillance*
NCDSB Policy
- E-30 Joint Transportation
- E-34 Safe Schools
- I-1 Video Surveillance
- I-2 Responsible Use of Information Communication & Technology
- P-24 Personal Information Management

NCDSB Administrative Procedure
- APE024-2 Breach of Personal Information

DEFINITIONS

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

Covert surveillance
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, including notes and photographs.

ICT Department
Information and Communication Technology Department of the Board

Personal information
Recorded information about an identifiable individual as per MFIPPA.

Reception equipment
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.

Storage device and recorded media
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.

Video surveillance equipment
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.

PROCEDURES

1.0 GENERAL PROVISIONS

1.1 All matters relating to the installation, use, and access of video surveillance shall be in compliance with relevant legislation and policies.

1.2 The use of video surveillance systems and the resulting records are used strictly for inquiries and proceedings related to maintaining the health, safety and well-being of students, staff, and visitors while on Board property and for the protection of school property.

1.3 The Principal is responsible for the proper implementation and control of the video surveillance system in a school.

1.4 The improper use of video surveillance systems will not be tolerated and will result in appropriate administrative or disciplinary action in any cases of wrongful use.

1.0 CONSIDERATIONS PRIOR TO USING A VIDEO SURVEILLANCE SYSTEM

2.1 Before deciding if a school or facility warrants a video security surveillance system, the Board should consider the following:

i) A video security surveillance system should only be considered after other measures of deterrence or detection have been considered and determined to be ineffective. Video surveillance should only be used once it has been determined that conventional methods of maintaining a safe and secure environment have proven not to provide the level of safety that is required.

ii) Verifiable and specific incidents of vandalism or safety concerns must exist prior to the installation of video surveillance equipment.

iii) The Board should ensure that the proposed design and operation of the video surveillance system minimizes privacy intrusion to that which is absolutely necessary to achieve its required and lawful goals.

2.2 Prior to implementing a video surveillance program, a school or facility should be able to demonstrate:

i) a history of incidents (e.g., intrusion, personal safety issues) occurring in the specific school / facility;
ii) the effect of the physical circumstances of the school/facility; and
iii) how a video security surveillance program would be effective in dealing with or preventing future incidents of the type that have already occurred.

3.0 INSTALLATION OF VIDEO SURVEILLANCE EQUIPMENT

3.1 A Supervisory Officer will authorize the installation of a video surveillance system in a school, upon the recommendation of the Principal and the Manager of Plant and Maintenance. Any change in camera location must be authorized in the same manner.

3.2 Video surveillance equipment shall not monitor the inside of areas where students, staff, and the public have a higher expectation of privacy (washrooms, change rooms, private offices).

3.3 Video surveillance equipment will only be installed by a designated NCDSB employee or third-party provider of the Board.

3.4 Video surveillance equipment should be installed in such a way that only spaces that have been identified as requiring video surveillance are monitored.

3.5 Cameras placed outside on a school site should be positioned only where it is necessary to protect external property and school assets or to provide for the personal safety of individuals on school grounds and premises.

3.6 Cameras should not be directed to look through windows of adjacent buildings or onto adjacent property.

3.7 If cameras are adjustable by operators, this practice should be restricted, if possible, so that operators cannot adjust or manipulate the cameras to overlook spaces that are not intended to be covered by the video surveillance system.

3.8 Maintenance of the cameras and the video surveillance equipment is the responsibility of the ICT Department with support from the Plant and Maintenance Department and the third party service provider of the Board.

3.9 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 ICT Department. Email techsupport@ncdsb.on.ca for any incidents associated to video surveillance systems and cameras.

3.10 The installation of video surveillance equipment by third-party service providers operating in our schools / facilities (tenants on Board property) must follow this procedure.

3.11 The installation of fake or dummy cameras is prohibited.

3.12 Video monitors should not be located in an area that allows for public viewing.

4.0 NOTIFICATION OF THE USE OF VIDEO SURVEILLANCE

4.1 Notice signs should be installed at all locations that use video surveillance systems in accordance with the notification requirements of MFIPPA.

4.2 The public, students, and staff members should be notified of video surveillance through clearly written signs prominently displayed in the main entrances of all Board facilities that operate a video surveillance system.

4.3 The NCDSB will endeavour to be as open as possible about the video surveillance system in operation and, upon request, will make available to the public information on the rationale for its use, objectives, and procedures that have been put in place.

4.4 Students and parents/guardians need to be informed by the Principal at the beginning of each school year that the Board may be recording student behaviour on school property and/or school buses and need to be informed about the purpose of such practices.

4.5 Principals will keep staff informed of the purpose of video surveillance and the limitations of viewing and accessing records.

4.6 A Supervisory Officer or designate will be responsible to ensure that service providers are aware of and comply with this administrative procedure when video surveillance equipment is used in a school, facility, or school bus.

5.0 STUDENT TRANSPORTATION

5.1 The Board may equip school buses and other school board vehicles which are owned, leased, contracted and/or operated by the Board with video recording devices for monitoring student behaviour.

5.2 Video recording devices may be in operation on a temporary basis or rotated between vehicles without prior notice to students, as deemed necessary by the Transportation Consortium.

5.3 Video recording devices may be installed on vehicles used for the transportation of students when the administrators have received complaints of inappropriate behaviour or have reason to believe that behaviour problems exist or are about to occur.

5.4 Any agreements between the Board and service providers shall state that the records dealt with or created while delivering a video surveillance system are under the Board's control and subject to the Acts.

5.5 Service providers and employees of service providers are required to review and comply with these procedures and the Acts in performing any duties and functions related to the operation of the surveillance system used on student transportation vehicles.

5.6 Bus operators, in consultation with the consortium, are responsible to audit the use and security of surveillance cameras on school buses.

6.0 USE, DISCLOSURE, RETENTION, SECURITY, AND DISPOSAL OF SURVEILLANCE RECORDS

6.1 Any information obtained through video surveillance systems may only be used for the purposes set out by MFIPPA and must relate to the protection of students, staff, and the public, including the discipline or consequences that arise from that, or it must assist in the detection and deterrence of criminal activity and vandalism. Information should not be retained or used for purposes other than those described above.

6.2 All recorded images are the property of the Board and are used, disclosed, retained, secured, and disposed of in accordance with MFIPPA.

6.3 Circumstances that warrant a review shall be limited to instances where an incident has been reported or observed or to investigate a potential crime.

6.4 Video surveillance should not be used for monitoring staff performance.

6.5 Reception equipment will be installed only in identified public areas where video surveillance is necessary to ensure the safety of staff, students, and school property. The equipment will operate up to 24 hours/7 days a week, within the limitations of the system.

6.6 The Principal or Site Supervisor should be responsible to manage, supervise, and audit the use and security of cameras, monitors, computers used to store images, or all other video records related to the site.

6.7 Video records may never be sold, publicly viewed, or distributed in any other fashion, except as provided by this policy and the appropriate legislation or as otherwise required by law or as evidence in a criminal or disciplinary proceeding.

6.8 Access to the storage devices should be limited to authorized personnel only.

6.9 Images collected should only be viewed by the Principal (or Vice-Principal) of the school, site manager, supervisory officer and/or in cooperation with members of the police.

6.10 Disclosure of video records should be on a need-to-know basis, in order to comply with the Board's policies, including the promotion of the safety and security of students, the protection of Board property, and deterrence and prevention of criminal activities.

6.11 A log should be maintained by the Principal, Site Manager, or designate of all episodes of access to or use of recorded materials, to provide for proper auditing and accountability purposes.

6.12 An individual whose personal information has been collected by a video surveillance system has the right of access to their personal information, unless an exemption applies. Access to an individual's own personal information in these circumstances may depend upon whether any exempt information can be reasonably severed from the record (for example, other individuals in the video would have to be severed from the record). Access to an individual's personal information in whole or in part may be refused where disclosure would constitute an unjustified invasion of another individual's privacy.

6.13 Parents, guardians, or employees requesting to view a segment of a video record involving their child(ren) or themselves may do so under the MFIPPA. However, the confidentiality of others must be considered and if the record cannot be severed, access will not be granted.

6.14 Only the Chief Executive Officer will authorize the release of video records to the police, upon receipt of a detailed, written request.

6.15 When surveillance records are released to the police or another authorized party, it is understood that the individual must comply with the applicable privacy legislation and holds responsibility for the security and privacy of the data accordingly.

6.16 Video surveillance monitors shall not be viewed in real time in order to enforce school rules unrelated to the purposes of this policy. Real-time viewing of camera monitors is only permissible for limited duration when required for specific safety and protection issues.

6.17 Vendors and/or service providers of the Board's video surveillance equipment should not have access to recorded information.

6.18 Recorded images that have not been viewed or used for investigation should be retained for a standard period of time, typically one month. Recorded information that has not been used in this fashion is to be routinely erased every 30 days in a manner in which it cannot be reconstructed or retrieved.

6.19 Recorded information that has been viewed or used in the investigation of an incident shall be retained for a period of one year from the date viewed or one year from the date of resolution of the incident.

6.20 Old storage devices must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved.

7.0 COVERT SURVEILLANCE

7.1 Covert surveillance occurs when surveillance devices are used without notification to individuals.

7.2 Cover surveillance shall only be used in specific limited circumstances as an investigative tool related to criminal or illegal activity.

7.3 This type of surveillance will only be used when all other methods of dealing with the situation have been exhausted, and following the completion of a comprehensive assessment of the privacy impacts.

7.4 Covert surveillance will only be used with the approval of the Director of Education and with the support of police services, for a limited period of time.

7.5 After a suspect has been identified, the surveillance equipment shall be removed.

8.0 ACCOUNTABILITY MEASURES

8.1 The Chief Executive Officer will facilitate regular reviews of these procedures in consultation with the appropriate school and system staff. Changes will be communicated in a timely manner to all those impacted.

8.2 Staff with responsibilities for the operation of the video surveillance system will receive training as to the permissible uses as detailed in this procedure.

8.3 The Board will ensure that the use and security of video surveillance systems is subject to regular audits.

8.4 The Board will regularly review and evaluate its video surveillance systems to ascertain whether it is still justified. This shall include an assessment of whether the deployment of cameras at a particular school remains justified. This evaluation shall occur at least once every three years and will include the review of the associated policy and administrative procedures.

8.5 In the event of a breach of privacy, the Principal or Site Supervisor will adhere to the related NCDSB policy and procedures, which includes but is not limited to:

i) Identify the scope of the potential breach and take steps to contain it;

ii) Identify those individuals whose privacy was breached and, barring exceptional circumstances, notify these individuals accordingly;

iii) Notify the appropriate Supervisory Officer.

9.0 RELATED FORMS AND DOCUMENTS

Nil.

Chief Executive Officer: *Tricia Stefanic Weltz*
Date: September 2025