



CAMERA SURVEILLANCE

Procedures

1.0 Purpose

This policy is developed for the purpose of implementing the objectives and law as maintained in the Municipal Freedom of Information and Protection of Privacy Act. It is not to be interpreted in any way as being inconsistent with the Act or as to limit or restrict the rights under the Act. The following are specific statements regarding the purpose of the policy:

- To establish the principles and mandatory requirements in order to maintain a safe environment.
- To protect the school property from theft or vandalism.
- To support the Administration in the identification of intruders and persons breaking the law.
- To establish a procedure to notify the public that the equipment is in place.
- To establish stringent privacy controls.
- To establish timelines for maintaining video.

2.0 Scope

This policy applies to all of the schools, Board offices, and Board properties, where surveillance cameras are installed.

Service providers of student transportation with surveillance cameras are to adhere to the policy.

3.0 Conditions

The Director of Education or Designate is responsible for the privacy obligation under the Municipal Freedom of Information and Protection of Privacy Act. The Director of Education or Designate will advise school administrators each year of the need to comply with the Act and Policy.

Board employees and service agencies (i.e. police) will have access to the personal information collected only where it is necessary to the performance of their duties and where the access is necessary and proper in the discharge of the Board's function. At all times, DSB Ontario North East maintains control of and responsibility for the video surveillance system and data produced.

3.1 Facilities

- Signs provided by the Board shall be clearly and prominently posted on all main doors of entrances notifying students, staff and community visitors of the surveillance cameras. These shall be displayed at all Board properties where surveillance cameras are in use.
- No school shall have cameras that are not connected to a recording device.

3.2 Camera Requests

- Requests for surveillance cameras must be submitted to the Superintendent of Education for consideration.
- Requests must designate the specific areas of installation and surveillance.
- Requests must include the name of the person authorized to operate the system.
- Times of operation of cameras will be defined.

3.3 Review

Each school who presently has camera surveillance, shall submit to the Board a review of the operational procedures for the compliance with this policy.

4.0 Storage, Retention and Disposal

The records dealt with or created by the video surveillance program are to be under the Board's control and are subject to the Acts.

4.1 Storage

Video is stored on a server in a locked room. Principals and Vice Principals access it through video surveillance software with their network credentials. Each storage device that has been used shall be dated and labelled. (Appendix A)

Access to the storage devices shall be limited to the Principal of the School or Designate. Logs shall be kept (Appendix A) of all instances of access to, and use of, recorded materials, and maintain an accurate audit trail.

4.2 Real-Time Viewing

The real-time viewing of the recorded information is limited to the Principal and a Designate. Circumstances that warrant a review should be limited to instances where an incident has been reported/observed or for investigation of a potential crime.

The real-time viewing of the monitors shall be by the Principal or a limited number of office individuals.

4.3 Retention

Recorded information that has been viewed for law enforcement, school or public safety purposes per Section 5 of Policy Regulation 823 under the Municipal Act requires that the personal information must be retained for one year.

The school shall store and retain information for evidentiary purposes according to the procedures until the law enforcement authorities request them.

4.4 Disposal

After time lapse of storage, the records must be securely disposed in a manner that personal information cannot be reconstructed. These methods may include burning, shredding or magnetically erasing of the personal information.

5.0 Complaints

Any complaints in regards to breach of the policy shall be directed to the Director of Education.

Any breach that is knowingly or deliberately enacted will be subject to discipline. The discipline will be a penalty up to and including termination.

6.0 Access to Information

6.1 Access to Personal Information

Any student, staff member or member of the public that has been recorded by a video surveillance camera has the right of access to his or her personal information under section 36 of the Municipal Act. The access may be granted by one's own personal information in whole, or part, unless an exemption applies under section 38 of the Municipal Act.

The heads of institutions (Principals) may refuse to disclose information to the individual to whom it relates if the disclosure would constitute an unjustified invasion of another individual's privacy (MFIPPA Section 38(b)).

Therefore, access to an individual's own personal information may depend on whether any exempt information can be reasonably severed from the record by such methods as digitally "blackening out" the images of other individuals whose images appear on the videotapes.

6.2 Access by Authorities

Requests for stored information shall be made using Appendix B. The form shall be completed before disclosure. This form will be monitored by the Principal or Designate.

7.0 Auditing and Evaluating the Use of Video Surveillance

The Superintendent of Education or designate, or the Building Services Manager, will perform periodic and/or spot audits of access to video surveillance systems and compliance with procedures.

8.0 Covert Surveillance

Covert surveillance occurs wherever surveillance cameras are set up without notification. The practice of covert surveillance is one that has the potential of being highly privacy-invasive and must only be used as a last resort in limited case specific circumstances.

All covert surveillance applications must be directed to the Superintendent of Human Resources for approval, and must clearly describe the rationale and the timelines for such action to be taken.

All covert surveillance will be time-limited.

Appendices

Appendix A: Video Archive Storage Log

Appendix B: Video Access Request Form

References

VIDEO ACCESS REQUEST FORM

Date of Request: _____

REQUESTOR DETAILS

Name of Requestor: _____

Under the Authority of: _____

REQUESTED INFORMATION

School: _____

Principal: _____

(In as much detail as possible, including date, time, individuals involved, specific location, as well as reason for request)

DETAILS OF REQUEST:

	ROUTING → Requestor → School Principal or Superintendent of Education → Communications Officer
Requestor Signature	

OUTCOME OF RELEASE TO AUTHORITY: (OFFICE USE ONLY)

--

Date of Tape: _____ Tape Number/Code: _____

 Approved Not Approved

Approver Name and Title_____
Approver Signature_____
Date

Date Returned: _____

OR

Date tape Destroyed after use: _____