PURPOSE

Surveillance equipment can be used by school boards/authorities to comply with responsibilities under the Education Act and the duties of its employees as set out in the Education Act and Regulations. School boards/authorities can use video surveillance and the resulting records for inquiries and proceedings related to maintaining the health, welfare and safety of students, staff, and visitors while on school board/authority property and the protection of school property.

Definitions

Personal Information - Recorded information about an identifiable individual which includes, but is not limited to, information relating to an individual's race, colour, national or ethnic origin, sex, and age.

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.

Record - Any information however recorded, whether in print form, on file, by electronic means or otherwise and including photographs, film, microfilm, videotape, machine-readable record, and any record that can be produced from a machine-readable record.

Video Surveillance System - A video, physical, or mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing, or monitoring of individuals in school buildings and on school premises (per IPC Video Surveillance Guidelines). Within the school board/authority, the surveillance system includes hand-held, portable digital devices used by principals and vice-principals to record school incidents for investigative purposes. Additional components of the surveillance system include portable video cameras that are used to record incidents
on designated school buses from time to time as required.

Storage Device - Refers to a video tape, computer disk or drive, CD-ROM, computer chip, or other device used to store the recorded data or visual, audio, or other images captured by a video surveillance system.

Considerations Prior to Using a Video Surveillance System

Before deciding if a school or facility warrants a video security surveillance system, the school board/authority should consider the following:

- A video security surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable. 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.
- Verifiable and specific incidents of vandalism or safety concerns must exist prior to the installation of video surveillance equipment.
- The school board/authority 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.

Notification of the Installation of a Video Surveillance System

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

Clearly written signs should be prominently displayed at the perimeter of surveillance areas so that students, staff, and the public have reasonable and adequate warning that surveillance is or may be in operation before entering any area under surveillance.

Signage will satisfy the notification requirements of the Acts, which include informing individuals of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information is intended to be used; and the title, business address, and telephone number of someone who can answer questions about the collection. At a minimum, there should be a sign in place that notifies individuals of the recording and informs them that they may contact the school office with any questions. The remainder of the notice requirements under the Acts can be satisfied through information pamphlets available in the school office.

The school board/authority should endeavour to be as open as possible about the video security surveillance program in operation and, upon request, will make available to the public information on the rationale for the video surveillance program, its objectives, and the policies and procedures that have been put in place.

Students need to be informed by the school principal at the beginning of each school year that the school board/authority may be recording student behaviour on school property and/or school buses and need to be informed about the purposes of such practices.

Where video surveillance is used on a school site, students, parents, and guardians shall be informed of related policies and procedures as incorporated into the student handbook or agenda.

Where video surveillance is used on a school site, all teaching and non-teaching staff shall be informed of related policies and procedures as incorporated into the staff handbook.

Teaching and non-teaching staff should be informed of the purpose of video surveillance and the constraints on viewing or distributing records.

Locations of Equipment

Reception equipment and/or surveillance equipment, such as video cameras, should only be installed in identified public areas where video surveillance is a necessary and viable means of ensuring the safety of students, staff, and school property or a necessary and viable means of detection or deterrence of criminal activity.

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

Cameras located internally should not be directed to look through windows to areas outside of the building.

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.

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

Video surveillance should not be used in locations where the students, staff, and public have a reasonable expectation of confidentiality and privacy, such as washrooms, change rooms, and private conference/meeting rooms. Cameras may be located in adjacent corridors to monitor traffic into these areas.

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 program.

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

Transportation Vehicles

A school board/authority may equip school buses and other school board/authority vehicles which are owned, leased, contracted and/or operated by the school board/authority with video recording devices for monitoring student behavior.

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 Manager of Transportation.

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.

Any agreements between the school board/authority and service providers shall state that the records dealt with or created while delivering a video surveillance program are under the school board's/authority's control and subject to the Acts.

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 transportation vehicles.

The Manager of Transportation or designate is responsible for establishing procedures to ensure that its employees and transportation service providers use, collect, secure, retain, and dispose of recorded information in accordance with this policy and the Acts.

Secure Transmission

Information transmitted by the video surveillance equipment must be transmitted in a secure manner.

Use a wired video surveillance system, which inherently prevents interception, or a wireless surveillance system with appropriate measures, such as strong encryption, to preclude unauthorized access.

Wireless communication technology is not to be used unless strong, privacy-protective precautions have been used.

Maintenance

The school principal or site manager is usually responsible for ensuring that all surveillance equipment is maintained and serviced regularly.

Imaging equipment should be periodically inspected to ensure that video cameras and recording equipment are operating properly according to manufacturers' specifications.

Any issues or concerns regarding the performance of such equipment should be followed up with immediately.

Use, Disclosure, Retention, Security, and Disposal of Surveillance Records

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.

All recorded images are the property of the school board/authority and are used, disclosed, retained, secured, and disposed of in accordance with MFIPPA.

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

Video surveillance should not be used for monitoring staff performance.

The school principal or site manager should be responsible to manage, supervise, and audit the use and security of cameras, monitors, tapes, computers used to store images, computer diskettes, or all other video records related to the site.

The Manager of Transportation or designate shall be responsible to audit the use and security of surveillance cameras on school buses, including monitors and tapes.

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

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

Images collected should only be viewed by the principal or vice-principal of the school, site manager, or the Superintendent of Education and/or in co-operation with members of the police.

The principal or site manager must authorize access to all video records other than those requested by the police. Without authorization by the principal or site manager, video records will only be released to or viewed by the police after school staff has been provided with a valid warrant.

When investigating specific incidents, the principal or vice-principal may enlist the aid of staff in the identification of individuals.

Disclosure of video records should be on a need-to-know basis, in order to comply with the school board's/authority's policy objectives, including the promotion of the safety and security of students, the protection of school board/authority property, and deterrence and prevention of criminal activities.

Video records may be released to third parties or applicants in conformance with the provisions contained in the *Freedom of Information and Protection of Privacy Act* (FIPPA) of Ontario and any rules or regulations thereunder or as otherwise required by law.

A log should be maintained by the principal, site manager, or designate of all episodes of access to or use of the recorded materials, to provide for a proper audit trail.

Recorded images shall be released to the police on request to aid in law enforcement in accordance with MFIPPA.

A storage device release form should be completed before any storage device is released to authorities or third parties. Any such release shall be made only in accordance with applicable legislation. The form will indicate the individual or organization who took the device, under what authority, when this occurred, and if it will be returned or destroyed by the individual or organization after use. This activity will be subject to audit and strictly enforced.

Video monitors for real-time monitoring shall be located in a protected area to prohibit unauthorized viewing by the public. Monitors can only be viewed by the principal, vice-principal, or designate. Real-time viewing of monitors may be delegated by the principal or Director of Education to a very limited number of individuals (e.g., a secretary or a special event security guard).

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.

Reception equipment should be located in a strictly controlled access area. Only controlling personnel or those properly authorized in writing by those personnel should have access to the controlled access area and the reception equipment.

Any agreements between the school board/authority and the service provider should state that the records dealt with or created while delivering a video surveillance program are under the school board's/authority's control and are subject to the Acts.

Vendors and/or service providers of the school board's/authority's video surveillance equipment shall not have access to recorded information.

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.

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.

The principal or site manager must ensure that video records are disposed of in a secure manner.

Old storage devices must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved. Destruction methods for tapes and diskettes may include magnetic erasure, shredding, or incineration.

The Storage Device Disposal Record shall be completed when disposing of a storage device.

All recorded tapes and other storage devices that are not in use should be stored securely in a locked receptacle located in a controlled-access area as designated by the school principal or site manager. Each storage device that has been used shall be dated and labeled with a unique identifier, sequential number, or other verifiable symbol.

Access to Personal Information

Individuals who have been recorded by surveillance systems have the right to request access to their personal information under the Acts.

Parents, guardians, or employees requesting to view a segment of a video record involving their child(ren) or themselves may do so under the *Freedom of Information and Protection of Privacy Act* legislation.

Access may be granted to one's own personal information in whole or in part, unless an exemption applies under MFIPPA or FIPPA.

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. Access to an individual's personal information in these circumstances may depend upon whether any exempt information, such as other individuals in the video, can reasonably be severed from the record.

Should it become necessary to allow a parent or guardian to view a videotape where the confidentiality of others must be protected, the following options will be considered:

- Seek permission from the other party(s)
- Digitally enhance the tape to block the identity of the person(s)

This viewing must be done in the presence of an employee designated by the superintendent. The parent has the right to request an advocate to be present.

Principals should consult with their superintendent and/or the Freedom of Information/Records Management Coordinator regarding requests for access.

Training of Staff

Training programs addressing staff obligations under the Act shall be conducted.

The school principal or site manager is responsible for ensuring that all staff with access to surveillance equipment are trained, comply with, and understand their obligations under the Acts and related procedures.

Staff with responsibilities for the operation of the video surveillance equipment will receive training as to the permissible uses and the protections against inadvertent disclosure or retention.

Auditing and Evaluating the Use of Surveillance

The school board/authority will ensure that the use and security of video surveillance equipment is subject to regular audits. These audits will address the school board's/authority's compliance with the operational policies, guidelines, and procedures. An external body may be retained in order to perform the audit. The school board/authority will endeavour to immediately address any deficiencies or concerns identified by the audit.

Employees and service providers should be aware that their activities are subject to audit and that they may be called upon to justify their surveillance interest in any given individual.

The school board/authority will regularly review and evaluate its video surveillance program 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/update of associated policy, procedures, and guidelines.

Covert Surveillance

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

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

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.

The benefits of capturing the information must outweigh the violation of privacy of the individuals observed. Covert surveillance will only be used with the approval of the superintendent of education and with the support of the police and will be time-limited.

Covert surveillance equipment shall be positioned in such a way as to minimize surveillance. For example, if equipment is being stolen or vandalized, individuals should only be recorded if they approach the equipment.

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

The school board/authority should develop a protocol that establishes how the decision to use covert surveillance is made on a case-by-case basis. The protocol would also include privacy protection practices for the operation of the system.

Privacy Breach Response

Any inadvertent disclosure of personal information must be reported immediately to the Freedom of Information/ Records Office, Director of Education.

Sample Notifications

The following sample might be posted in main entrance of the school:

THE USE OF VIDEO SURVEILLANCE IS IN EFFECT

Surveillance systems are in operation to reduce/prevent vandalism, theft and violence and to ensure the safety of students, staff and others.

Information collected is collected by the *School Board* under the authority of the *Education Act* in accordance with the Municipal Freedom of Information and Protection of Privacy Act. For information, contact the school principal or the Freedom of Information/Records Management Coordinator of the *School Board, address, (XXX) XXX-XXXX - ext XXXX.*

Notice in Facilities

Entrances other than the main entrance, fence signage, and notification in facilities shall be:

THE USE OF VIDEO SURVEILLANCE IS IN EFFECT

Questions regarding this surveillance should be directed to the principal of the school.

Notice in School Handbook - Secondary

The *School Board* uses surveillance equipment used in secondary school facilities and school buses to:

a) enhance the safety of students and staff;

b) protect school property against theft or vandalism;

c) aid in the identification of intruders and of persons who endanger the health, well-being, or safety of school community members.

Information collected is collected by the *School Board* under the authority of the Education Act in accordance with the Municipal Freedom of Information and Protection of Privacy Act. For information, contact the school principal or the Freedom of Information/Records Management Coordinator of the *School Board, address, (XXX) XXX-XXXX - ext XXXX.*

Notice in School Handbook - Elementary

School board buses may from time to time use video surveillance as required.

FORM A
Log Sheet – Viewing of Recorded Images

	Date of Viewing (yyyy/mm/dd)	Date Recorded (yyyy/mm/dd)	Tape No./ ID #	Camera No./ Name	Surveillance Period	Type of Incident Reviewed	Incident Saved to Computer HD/CD-R /VCR	Police Notified of the Incident	Name of Person Viewing Recorded Images	Signature of Person Viewing Recorded Images
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Audit Conducted (Date/Time): _____

Auditor (Name – Printed): _____

Audit Organization (Name – Printed): _____

Signature of Lead Auditor: _____

FORM B
Log Sheet – Recorded Images Removed from School/Location via CD-R, Printed Copy, or VCR Cassette

	Date Removed (yyyy/mm/dd)	Date Recorded (yyyy/mm/dd)	Tape No./ ID #	Camera No./ Name	Surveillance Period	Type of Incident	Format of Image (CD-R, VCR Cassette, Print	Officer Name/ Badge/Occ #	Police Officer's Signature	Name and Signature of Person Releasing the Information
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Audit Conducted (Date/Time): _____

Auditor (Name – Printed): _____

Audit Organization (Name – Printed): _____

Signature of Lead Auditor: _____

FORM C
Log Sheet – Disposal of Recorded Information

	Date of Disposal (yyyy/mm/dd)	Time of Disposal	Date Recorded (yyyy/mm/dd)	Tape No./ ID #	Camera #/ Name	Surveillance Period	Type of Incident	Type of Device (CD-R, VCR tape)	Method of Disposal	Name of person disposing of recorded information	Signature of person disposing of recorded information
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

Not applicable for the routine overwrite/erasure of unviewed recorded material.

School Or Facility: _____

Audit Conducted (Date/Time): _____

Auditor (Name – Printed): _____

Audit Organization (Name – Printed): _____

Signature of Lead Auditor: _____

VIDEO SECURITY SURVEILLANCE SYSTEM STORAGE DEVICE RELEASE FORM

Date (yyyy/mm/dd)	**Time**	**Storage Device ID #**	**Form #**
Name of School/Facility	**Location of Storage Device** ☐ In-Use _____ ☐ Used _____	**Type of Device** ☐ Tape ☐ CD ☐ Disk ☐ Other (Specify) _____	
Name of Authorized Board Individual Releasing Storage Device (Print) **Position**		**Signature**	
Name of Individual Taking Custody of Storage Device (Print)		**Signature**	
Position	**ID or Badge Number**	**Organization and Telephone Number**	
Purpose or Reason For Release			
Disposition Following User: ☐ To Be Destroyed	☐ To Be Returned to School/Facility of Origin ☐ Other (Specify) _____		

An individual Storage Device Release Form is to be completed for each device to be released.
Copies to be made and distributed as required.

References

1. Information and Privacy Commissioner - *Guidelines for Using Video Surveillance Cameras in Schools* (2003)
2. Simcoe County District School Board - *Surveillance Systems, Administrative Procedures*
3. Windsor-Essex Catholic District School Board - *Video Security Surveillance Policy*
4. Kawartha Pine Ridge District School Board - *Video Surveillance, Administrative Regulations*
5. Avon Maitland District School Board - *Video Surveillance, Administrative Procedure No. 525*