Administrative Procedure: Video Surveillance

Table of Contents

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 or including photographs, film, microfilm, videotape, machine-readable record, and any record that can be produced from a machine-readable record.

Video Surveillance - A video, physical, or mechanical, electronic or digital surveillance

System (VSS) - system or device that enables continuous or periodic video recording, observing, or monitoring of individuals in school buildings and on school premises. Within the Board authority, the surveillance system includes hand-held, portable digital devices used by principals or other supervisors to record 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 videotape, 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 (VSS)

A video security surveillance system will be considered only after other measures of deterrence or detection have been considered and rejected as unworkable, and only after it has been determined that conventional methods of maintaining a safe and secure environment have proven not to provide the level of safety required.

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

The Board shall ensure that the proposed design and operation of the VSS minimizes privacy intrusion to that which is absolutely necessary to achieve its required and lawful goals.

Notification Of The Installation Of A VSS

The school shall notify the public, students and staff about a VSS through clearly written signs prominently displayed in the main entrances of all the facilities that operate a VSS.

Clearly written signs shall 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 include:

- The legal authority for the collection of personal information.
- The principal purpose for which the personal information is intended to be used.
- 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 are satisfied through information pamphlets available at the school office.

The Board will be as open as possible about the VSS program in operation and, upon request, will make available to the public information on the rationale for the VSS program, its objectives, and the policies and procedures that have been put in place.

Schools shall be informed by the school principal at the beginning of each school year that the Board may be recording student behaviour on school property and/or school buses, and shall be further informed about the purposes of such practices.

Where a VSS is used on a school site, students, parents, and guardians, shall be informed of related policies and procedures in the student handbook. Teaching and non-teaching staff shall be informed of related policies and procedures as incorporated into the staff handbook, as well as 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 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 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.

A VSS should not be used in locations where students, staff and the 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 VSS.

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

Use of VSS Equipment

Only the school principal, or designate, or senior Board staff employees will be authorized to operate the system.

Video surveillance will be in place and operating 24 hours a day, all year long.

The Manager of Operations, or designate, will be responsible for the Board's privacy obligations under the Acts and its policy. This individual should also be responsible for advising staff at each school of the need to comply with the Acts.

Board employees and service providers will have access to the personal information collected under the program only where necessary in the performance of their duties, and where the access is necessary and proper in the discharge of the Board's functions.

Employees will be subject to discipline for knowingly or deliberately breaching the policy or the provisions of the Acts or other relevant statutes.

This policy will be incorporated into the training and orientation programs of the Board.

Use, Disclosure, Retention, Security & Disposal of Video Surveillance Records

Any information obtained through video surveillance systems may only be used for the purposes set out in this policy 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 in this policy.

Video surveillance will not be used for monitoring staff performance.

All tapes or other storage devices that are not in use should be stored securely in a locked receptacle located in a controlled access area. Each storage device that has been used should be dated and labelled with a unique, sequential number or other verifiable symbol.

Access to the storage devices should be limited to authorized personnel. Logs should be kept of all instances of access to, and use of, recorded material, to provide for a proper audit trail.

The review of the recorded information is limited to the school principal, designated alternate, or senior Board staff employees. Circumstances that warrant a review should

be limited to instances where a serious incident has been reported/observed or to investigate a potential crime.

Information that has not been viewed for the purpose of protecting student safety or to deter, detect, or assist in the investigation of criminal activity should not be retained beyond one month. Unused tapes that are not viewed should be erased on a schedule not exceeding one month.

When recorded information has been viewed for the purpose of protecting student safety or to deter, detect, or assist in the investigation of criminal activity, Section 5 of Ontario Regulation 823 under the Municipal Act [Section 5(1)] of Ontario Regulation 460 under the provincial Act, requires that personal information that has been used must be retained for one year. If not used, the personal information may only be retained until dismissed from the investigation.

Each school must store and retain storage devices required for evidentiary purposes according to standard procedures until the law enforcement authorities request them. A storage device release form, or an entry in a log book, should be completed before any storage device is disclosed to the appropriate authorities. The form should indicate who took the device, under what authority, when this occurred and if it will be returned or destroyed after use. This activity should be regularly monitored and strictly enforced. Electronic logs should be kept where records are maintained electronically.

Old storage devices must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved. Disposal methods could include overwriting electronic records, shredding, burning or magnetically erasing the personal information.

Access To Personal Information

Any individual whose personal information has been recorded by a video surveillance system has a general right of access to his or her personal information under section 36 of the Municipal Act (Section 47 of the Provincial Act).

Access may be granted to one's own personal information in whole or in part, unless an exemption applies under Section 38 of the Municipal Act.

One exemption that may apply is contained in Subsection 38(b) of the Municipal Act, which grants the heads of institutions the discretionary power to refuse access where disclosure would constitute an unjustified invasion of another individual's privacy.

What To Do If A Privacy Breach Occurs

A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are not in accordance with the provisions of the Acts. Among the most common breaches of personal privacy is the unauthorized disclosure of personal information.

If an individual believes that the Board has failed to comply with one or more of the privacy protection provisions of the Acts, and that his or her privacy has been compromised as a result, the individual can file a complaint with the Information and Privacy Commissioner/Ontario (IPC).

Upon learning of a privacy breach, immediate action should be taken.

When faced with a potential breach of privacy, the first two priorities are:

Containment: Identify the scope of the potential breach and take steps to contain it

- Retrieve the hard copies of any personal information that has been disclosed.
- Ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information and obtain the individual's contact information in the event that followup is required.
- Determine whether the privacy breach would allow unauthorized access to any other personal information and take whatever necessary steps are appropriate (e.g. change passwords, identification numbers and/or temporarily shut down a system).

Notification: Identify those individuals whose privacy was breached and, barring exceptional circumstances, notify those individuals accordingly

- Notify the individuals whose privacy was breached, by telephone or in writing.
- Provide details of the extent of the breach and the specifics of the personal information at issue.
- Advise of the steps that have been taken to address the breach, both immediate and long term.

- Advise that the IPC has been contacted to ensure that all obligations under the Act are fulfilled.

Additional Steps

- Ensure appropriate staff within your organization are immediately notified of the breach, including the Freedom of Information and Privacy Coordinator, the Director of Education and School Principal.
- Inform the IPC registrar of the privacy breach and work together constructively with IPC staff.
- Conduct an internal investigation into the matter, linked to the IPC's investigation. The objectives of the investigation are to: 1) ensure the immediate requirements of containment and notification have been addressed; 2) review the circumstances surrounding the breach; and 3) review the adequacy of existing policies and procedures in protecting personal information.

Transportation Vehicles

The use of any VSS will be reviewed and governed by the Transportation Consortium. The Manager with responsibility for transportation, or designate, is responsible for establishing procedures to ensure that employees and transportation service providers use, collect, secure, retain, and dispose of recorded information in accordance with this policy and the Acts.