

YORK CATHOLIC DISTRICT SCHOOL BOARD



BOARD POLICY	
<i>Policy Section</i> Facilities	<i>Policy Number</i> 705
<i>Former Policy #</i> 512	<i>Page</i> 1 of 6
<i>Original Approved Date:</i> March 9, 2004	<i>Last Approval Date:</i> June 8, 2010

POLICY TITLE: USE OF SURVEILLANCE EQUIPMENT

SECTION A

1. PURPOSE

The York Catholic District School Board is committed to maintaining safe and secure environments for students, staff and community members by monitoring internal and external facility security and student behaviour. As such, the Board approves the installation and use of video security surveillance systems in schools and on Board premises. The purpose of this policy is to provide direction and guidelines to staff with respect to the installation and use of such systems.

2. POLICY STATEMENT

It is the policy of the York Catholic District School Board to employ video surveillance systems in schools and facilities owned by the Board and to operate these systems in compliance with legislation and guidelines of this policy.

3. PARAMETERS

- 3.1 Surveillance activities involving the collection, retention, use, disclosure and disposal or personal information in the form of video surveillance shall be in compliance with legislation including the *Privacy Impact Assessment Tool (Government of Ontario)*.
- 3.2 Video surveillance equipment will be installed for the purpose of ensuring the ongoing safety of students, staff, community members and property.
- 3.3 The equipment will be installed in such a manner that it monitors only the spaces requiring video surveillance.
- 3.4 Access to the school-based video surveillance equipment will be restricted to authorized individuals only (the School Principal or designate).
- 3.5 Monitoring of locations where students, staff or authorized visitors have an expectation of privacy (change rooms, washrooms, staff rooms) will be prohibited.

3.6 Video surveillance notification signs will be prominently displayed where there is video surveillance.

3.7 The Board will not be responsible for any breach of security or for the actions of others with respect to the use or misuse of video surveillance equipment.

4. RESPONSIBILITIES

4.1 Director of Education/Designate

- To oversee the Board video surveillance program

4.2 Manager of Facilities Services

- To oversee the life cycle management of the authorized video surveillance system.

4.3 Principal/Designated Employees

- To oversee the day to day operation of the video surveillance system in accordance with the policy, guidelines, and direction/guidance that may be issued from time to time.
- To report system failure or malfunction as soon as possible.

5. DEFINITIONS

5.1 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.
- The contents of a video surveillance system displaying the characteristics of an identifiable individual or the activities in which he or she is engaged will be considered "personal information" as defined under the Municipal Freedom of Information and Protection of Privacy Act.

5.2 Privacy Impact Assessment Tool

- A process used to evaluate privacy implications of information systems.

5.3 Record

- Any record of information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a videotape, a CD or DVD a machine-readable record, and any record that is capable of being produced from a machine-readable record.

5.4 Video Surveillance System

- A video, physical or other mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing or monitoring of personal information about individuals in open, public spaces (including streets, highways, parks). The term video surveillance system includes an audio device, thermal imaging technology or any other component associated with capturing the image of an individual.

5.4 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.

5.5 Storage Device

- 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.

6. CROSS REFERENCES

Municipal Freedom of Information and Protection of Privacy Act

Guidelines for Using Video Surveillance Cameras in Schools issued by the Information and Privacy Commissioner/Ontario, December 2003

YCDSB Policy 112 Privacy and Personal Information Management
YCDSB Policy 109 Records Management

POLICY TITLE: USE OF VIDEO SURVEILLANCE CAMERAS

SECTION B

GUIDELINES

1. General

Video security surveillance systems are a resource used by the York Catholic District School Board to promote the safety of pupils, staff and community members and to monitor internal and external facility security and student behaviour. In the event of a reported or observed incident, the review of recorded information may be used to assist in the investigation of the incident.

The Board will maintain control of and responsibility for the video surveillance system at all times. Any agreements between the Board and service providers shall state that the records dealt with or created while delivering a video surveillance program are under the Board's control and subject to the Municipal Freedom of Information and Protection Act (the Act).

2. Collection of Personal Information Using a Video Surveillance System

Any recorded data or visual, audio or other images of an identifiable individual qualifies as "personal information" under the Act. Video surveillance systems can be operated to collect personal information about identifiable individuals. The Board has the authority to collect this personal information in accordance with the Act.

3. The Design, Installation and Operation of Video Surveillance Equipment

In designing, installing and operating a video surveillance system, the Board will consider the following:

- 3.1 Staff will endeavour to 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, lawful goals.
- 3.2 Reception equipment such as video cameras, or audio or other devices will be installed in areas where video surveillance is a necessary and viable detection or deterrence strategy. The equipment will operate 24 hours/seven days a week.
- 3.3 The equipment should be installed in such a way that it only monitors those spaces that have been identified as requiring video surveillance. Cameras should not be directed to look through the windows of adjacent buildings.
- 3.4 If cameras are adjustable by operators, this should be restricted, if possible, so that operators cannot adjust or manipulate them to overlook spaces that are not intended to be covered by the video surveillance.
- 3.5 Equipment should never monitor the inside of areas where the students, staff and the public have a higher expectation of privacy (e.g. change rooms and washrooms).
- 3.6 Clearly written signs, prominently displayed at the entrances, exterior walls and/or the interior of buildings having video surveillance systems, shall provide students, staff and the public reasonable and adequate warning that video surveillance is in effect.

4 Access, Use, Disclosure, Retention, Security and Disposal of Video Surveillance Records

Any information obtained by way of video surveillance systems may only be used for the purposes of the stated rationale and objectives set out to protect student, staff and public safety or to detect and deter criminal activity and vandalism. Information should not be retained or used for any other purposes. Since video surveillance systems create a record by recording personal information, each school/facility having a system will implement the following procedures:

- 4.1 All CDs or DVDs or other storage devices that are not in use should be stored (quarantined) securely in a locked receptacle located in a controlled-access area, as determined by the Board. Each storage device should be dated and labelled (preferably with a unique, sequential number or other variable symbol). Access to the storage devices should only be by authorized personnel. Logs should be kept of all instances of access to, and use of, recorded material to enable a proper audit trail.
- 4.2 Procedures on the use and retention of recorded information include:
 - 4.2.1 Only authorized personnel including the principal or designate may review recorded information. Circumstances, which would warrant review, will normally be limited to an incident that has been reported/observed or to investigate a potential crime.
 - 4.2.2 The retention period for information that has not been viewed for law enforcement, school or public safety purposes shall be thirty (30) calendar days. Recorded information that has not been used within these timeframes, is to be routinely erased in a manner in which it cannot be reconstructed or retrieved.
 - 4.2.3 When recorded information has been viewed for law enforcement or school/public safety purposes the retention period shall be one (1) year from the date of viewing.
- 4.3 The Board will store and retain storage devices required for evidentiary purposes according to standard procedures until the police request them. A storage device release form will be completed before any storage device is disclosed to appropriate authorities. The form will indicate the name and pertinent facts of the individual to whom the device was given, under what authority, when this occurred, and if it will be returned or destroyed after use.
- 4.4 Old storage devices must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved. Disposal methods include shredding, burning or magnetically erasing the personal information.
- 4.5 An individual whose personal information has been collected by a video surveillance system has a right of access to his or her personal information. Access may be granted in whole or in part, unless an exemption applies under the Act. Access to an individual's own personal information in these circumstances may also depend upon whether any exempt information can be reasonably severed from the record.

- 4.6 The application of the frivolous or vexatious request provisions of the *Act* would occur in very rare circumstances. It can be concluded that a request for access to a record or personal information is frivolous or vexatious if:
 - 4.6.1 the opinion is, on reasonable grounds, that the request is part of a pattern of conduct that amounts to an abuse of the right of access or would interfere with the operations of the school/facility, or
 - 4.6.2 The opinion is, on reasonable grounds, that the request is made in bad faith or for a purpose other than to obtain access.

5. Training

Where applicable and appropriate, the policy and guidelines will be incorporated into training and orientation programs of the Board. Training programs addressing staff obligations shall be conducted as necessary.

6. Auditing and Evaluating the Use of a Video Surveillance System

The use and security of video surveillance equipment is subject to regular internal audits. The audit will address compliance with the operational policies, guidelines and procedures.

Approval by Board	<i>Date</i>
Effective Date	<i>Date</i>
Revision Dates	<i>Date</i>
Review Date	June 2015 <i>Date</i>