# Brant Haldimand Norfolk Catholic District School Board

## POLICY: VIDEO SECURITY SURVEILLANCE

| | | | |
|---|---|---|---|
| **Adopted:** | **02/22/05** | **Policy No:** | **400.11** |
| **Revised:** | **mm/dd/yy** | **Policy Category:** | **Operations** |

**Policy Statement:**

The Brant Haldimand Norfolk Catholic District School Board and its schools/sites will strive to maintain safe and secure learning environments for students, staff and community members involved in school programs.

In keeping with the Board's Safe Schools Policy, it is the Board's practice to use video security surveillance systems at schools and facilities, owned by the Board or on buses operated on behalf of the Board, as deemed necessary by the Director of Education.

**Policy Criteria:**

- All video surveillance equipment must be approved by the Associate Director, Corporate Services and Treasurer or an appointed designate.
- Principals, the Manager of Facilities and Construction Projects and/or other designated employees at schools and facilities with video security surveillance, are authorized to operate the systems.
- The Supervisor of Transportation and/or bus operators are authorized to operate video surveillance systems on student transportation vehicles.
- Board employees and service providers are to review and comply with the Policy, Administrative Procedures, and relevant Acts in performing their duties and functions related to the operation of the video surveillance system.
- Cameras will be positioned to only record identified public areas.
- Video security surveillance systems complement other means being used to promote and foster a safe and secure learning environment under the *Safe School Act.*
- Surveillance activities involving the collection, retention, use, disclosure and disposal of personal information in the form of video surveillance must be in compliance with the *Freedom of Information and Protection of Privacy Act.*
- The Brant Haldimand Norfolk Catholic District School Board will maintain control of, and responsibility for, the video surveillance system at all times

**Glossary of Key Policy Terms:**

**Personal information** is defined as 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. A simple image on a video surveillance system that is clear enough to identify a person, or activities in which he or she is engaged in, will be classified as "personal information" under the *Act*.

**Record** means 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 machine-readable record, and any record that is capable of being produced from a machine-readable record.

**Video Surveillance System** refers to a video, DVR (digital video recorder), physical or other 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. The Information and Privacy Commissioner/Ontario includes in the term video surveillance system thermal imaging technology or any other component associated with recording the image of an individual.

**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.

**Storage Device** refers to a videotape, computer disk or drive, CD-ROM, computer chip, DVR (digital video recorder) or other device used to store the recorded data or visual, audio or other images captured by a video surveillance system

**Statutory / Regulatory / Related Board Policy Linkages:**

The Education Act
The Freedom of Information and Protection of Privacy Act
Guidelines for Using Video Surveillance Cameras in Schools, December 2003

# Brant Haldimand Norfolk Catholic District School Board

## ADMINISTRATIVE PROCEDURES: VIDEO SECURITY SURVEILLANCE

| | | | |
|---|---|---|---|
| **Adopted:** | **02/22/05** | **Policy No:** | **400.11** |
| **Revised:** | **mm/dd/yy** | **Policy Category:** | **Operations** |

1. **Responsibilities:**

***Director of Education*** - is responsible for the overall Board video security surveillance program.

***Manager of Facilities and Construction Projects*** - is responsible for the development and review of the policy & supporting guidelines along with the technical aspects of the video security surveillance systems and the coordination of related audits. The Manager of Facilities and Construction Projects is also responsible for the life-cycle management of authorized video security surveillance systems (specifications, equipment standards, installation, maintenance, replacement, disposal, and related requirements (e.g. signage)) and Principal/Facility Manager/Operator training at Board sites.

***Coordinator of Communications*** - is responsible for the Board's privacy obligations under the *Acts* and the policy.

***Principal/Facility Manager*** - is responsible for the day-to-day operation of the system in accordance with the policy, guidelines, and direction/guidance that may be issued from time-to-time.

***Supervisor of Transportation*** - is responsible for the operation of video surveillance systems on student transportation vehicles.

***Board Solicitor*** - is responsible for the provision of legal advice related to the Board's obligations under the *Acts*.

2. **General**
   Video security surveillance systems are a resource used by the Brant Haldimand NorfolkCatholic District School Board at selected schools and sites within the Board's jurisdiction to promote the safety of pupils, staff, and community members. 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 security 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 *Acts*.

   These Guidelines do not apply to "covert surveillance". Covert surveillance refers to surveillance conducted by means of hidden devices, without notice to the individuals being monitored. This type of surveillance should only be used as a last resort in time limited, case-specific circumstances. Prior to deciding to use covert surveillance, a comprehensive assessment of the privacy impacts associated with the implementation of such a program shall be made. An example of a situation in which time-limited covert surveillance may be justified is where there is an ongoing problem of computer theft from a school's computer room. Covert surveillance equipment may be installed in order to identify the thief.

3. **Collection of Personal Information Using a Video Surveillance System**
   Any recorded data or visual or other images of an identifiable individual qualifies as "personal information" under the *Acts.* Video security surveillance systems can be operated to collect personal information about identifiable individuals. The Board has determined that it has the authority to collect this personal information in accordance with the *Act.* Pursuant to section 38(2) of the provincial *Act,* no person shall collect personal information on behalf of the Board unless the collection is expressly authorized, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity. The Board must be able to demonstrate that any proposed or existing collection of personal information by a video surveillance system is authorized under this provision of the *Acts*.

4. **Planning Considerations for Video Security Surveillance Systems**
   Before deciding if a school or facility warrants a video security surveillance system, the Board will consider the following:
   (a) A video security surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable.
   (b) Video surveillance should only be used where conventional means are substantially less effective than surveillance or are not feasible, and the benefits of

surveillance substantially outweigh the reduction of privacy inherent in collecting personal information using a video surveillance system.

(c) The acquisition, installation, and operation of individual video security surveillance systems should be justified on the basis of verifiable, specific reports of incidents of crime, vandalism or significant safety concerns.

(d) An assessment should be conducted of the effects that the proposed video surveillance system may have on personal privacy, and the ways in which any adverse effects can be mitigated. The Board shall utilize the Ontario Government's Privacy Impact Assessment tool.

(e) Consultations should be conducted with relevant stakeholders as to the necessity of the proposed video security surveillance program at the school/facility.

(f) The Board will endeavour to ensure that the proposed design and operation of the video security surveillance system minimizes privacy intrusion to that which is absolutely necessary to achieve its required, lawful goals.

5. **The Design, Installation and Operation of Video Security Surveillance Equipment in Buildings**

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

(a) Reception equipment such as video cameras, or other devices, should only be installed in identified public areas where video surveillance is a necessary and viable detection or deterrence activity. The equipment will operate up to 24 hours/seven days per week, within the limitations of system capabilities (e.g. digital, tape), power disruptions and serviceability/maintenance.

(b) 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.

(c) 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 program.

(d) Consideration should be given to the use of motion detectors to limit the time when the video surveillance cameras are in operation.

(e) Equipment should never monitor the inside of areas where students, staff, and the public have a higher expectation of privacy (e.g., change rooms and washrooms).

(f) Clearly written signs, prominently displayed at the entrances, exterior walls, and/or the interior of buildings having video security surveillance systems, shall provide students, staff, and the public reasonable and adequate warning that video surveillance is in effect. Signage will satisfy the notification requirements under section 39(2) of the provincial Act 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. This information can be provided at the location on signage and/or by other means of public notification such as pamphlets. Principals will be the Point-of-Contact for schools and Facility Managers will be the Point-of-Contact for non-school facilities.

(g) The Board will 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. This may be done in pamphlet or leaflet form. The Policy and Administrative Procedures will be posted on the Board's Web site.

(h) Reception equipment should be in a strictly controlled access area. Only controlling personnel, or those properly authorized, in writing, by those personnel according to the institution's policy, should have access to the controlled access area and the reception equipment. Video monitors should not be in a position that enables public viewing.

(i) Service providers should visit schools and facilities three to four times per year to ensure that video cameras, including image refocusing and lens cleaning, are operating properly. Any issues or concerns regarding the performance of such equipment should be followed-up with immediately.

6. **The Use and Operation of Video Security Surveillance Equipment in Transportation Vehicles**

(a) A vehicle that is equipped with video cameras shall display a warning sign advising students that they are subject to video surveillance.

(b) Storage devices (i.e., videotapes) currently being used on a transportation vehicle shall not be left in the vehicle overnight, with the exception of cameras that are secured and locked in a black box on the vehicle, and must be maintained in a secure location by the driver.

(c) Any storage device that has been used will be dated and labeled with the Bus Route #. Storage devices containing data and waiting to be recycled for further use will be maintained in a secure location by the school transportation contractor.

(d) Storage devices are the property of Transportation Services on behalf of the Boards served.

(e) Storage devices (i.e., videotapes) will be purchased by Transportation Services on behalf of the Boards served.

(f) The content of a storage device may be used to provide evidence to cause student discipline, i.e., suspension or expulsion. A storage device can be viewed by a student and his/her parent/guardian if:

i. all third parties (i.e., those whose images appear on the record) give permission for the record to be viewed, or

ii. the images of other individuals who appear on the record (storage device) are severed from the record (i.e., digitally “blacking out”).

7. **Access, Use, Disclosure, Retention, Security and Disposal of Video Security Surveillance Records**

Any information obtained by way of video security surveillance systems may only be used for the purposes of the stated rationale and objectives set out to protect students, 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 security surveillance systems create a record by recording personal information, each school/facility having a system will implement the following procedures:

(a) 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. Access to storage devices should be limited to authorized personnel. Each storage device that has been used should be dated and labeled with a unique, sequential number or other verifiable symbol. The *In-Use/Used Storage Device Register* (Appendix A) is to be used. Access to the storage devices should only be by authorized personnel. Logs (*Access to and Viewing of Recorded Material Log*) (Appendix B) should be kept of all instances of access to, and use of, recorded material to enable a proper audit trail.

(b) Procedures on the use and retention of recorded information include:

i. Only the Principal/Facility Manager and a delegated Alternate (designated by name and position, e.g., Vice-Principal or another Principal) and/or the Transportation Services Manager and a delegated Alternative (designated by name and position) may review the information. Circumstances, which would warrant review, will normally be limited to an incident that has been reported/observed or to investigate a potential crime. Real-time viewing of monitors may be delegated by the Principal/Facility Manager to a very limited number of individuals (e.g., a secretary, a special event security guard).

ii. The retention period for information that has not been viewed for law enforcement, school or public safety purposes shall be thirty-one calendar days. These time frames are based on experience, risk assessment, privacy considerations, and equipment capabilities. Recorded information that has not been used in this fashion, within these time frames, is then to be routinely erased in a manner in which it cannot be reconstructed or retrieved.

iii. 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. If personal information is used for this purpose, section 5(1) of Ontario Regulation 460 under the provincial *Act* requires the recorded information to be retained for one year.

(c) The Board will 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 (*Storage Device Release Form*) (Appendix C) will be completed before any storage device is disclosed to appropriate authorities.

The form will indicate who took the device, under what authority, when this occurred, and if it will be returned or destroyed after use. This activity will be subject to audit.

(d) 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 shredding, burning or magnetically erasing the personal information. The *Storage Device Disposal Record* (Appendix D) is to be completed.

(e) An individual whose personal information has been collected by a video surveillance system has a right of access to his or her personal information under section 47 of the provincial *Act* and section 36 of the municipal *Act*. Procedures must recognize this right. Access may be granted to one's own personal information in whole or in part, unless an exemption applies under section 49 of the provincial *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.

(f) The application of the frivolous or vexatious request provisions of the municipal *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:

i. 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

ii. the opinion is, on reasonable grounds, that the request is made in bad faith or for a purpose other than to obtain access.

(g) Principals/Facility Managers will respond to any inadvertent disclosures of personal information based on direction provided by the Coordinator of Communications. Any breach of the *Acts* shall be reported to the Coordinator of Communications.

8. **Training**

Where applicable and appropriate, the policy and guidelines will be incorporated into training and orientation programs of the Board and service provider(s). Training programs addressing staff obligations under the *Act* shall be conducted as necessary.

9. **Auditing and Evaluating the Use of a Video Surveillance System**

The Board will ensure that the use and security of video surveillance equipment is subject to regular audits. The audit will address the Board's compliance with the operational policies, guidelines and procedures. The audit will be conducted under the direction of the Associate Director, Corporate Services and may include the retention of an external consultant. The audit will normally review the following:

- Policy and Administrative Guidelines.
- Interior/exterior signage.

- Location of cameras.
- Individuals having access to equipment, monitors, etc.
- Security, location and storage of equipment, storage devices, etc.
- Maintenance and completeness of records, logs and forms.
- Vendor access.
- Requests for access to personal information.

The Board will endeavour to address immediately 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 program to ascertain whether it is still justified in accordance with the requirements in Paragraph 3. This evaluation shall occur at least once every three years and will include the review/update of the policy and the guidelines.

**Appendix A**

**The Brant Haldimand Norfolk Catholic District School Board**

Video Security Surveillance System

# IN-USE/USED STORAGE DEVICE REGISTER

| IN-USE STORAGE DEVICE | | | USED STORAGE DEVICE | | |
|---|---|---|---|---|---|
| **ID#** | **Type of Device (Tape, CD, etc.)** | **Location** | **ID#** | **Type of Device (Tape, CD, etc.)** | **Location** |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

School or Faculty _____Page _____of_____

Conducted (Date/Time): _____

Auditor's Name (Print Name): _____

Audit Organization (Print Name): _____

Signature of Lead Auditor: _____

**Appendix B**

# The Brant Haldimand Norfolk Catholic District School Board

Video Security Surveillance System

## ACCESS TO AND VIEWING OF RECORDED MATERIAL LOG

| ID # | Type of Device (Tape, CD, etc.) | Date of Viewing | Accessed By | Purpose of Access or Viewing | Signature |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

School or Faculty _____ Page _____ of _____

Audit Conducted (Date/Time): _____

Auditor's Name (Print Name): _____

Audit Organization (Print Name): _____

Signature of Lead Auditor: _____

**Appendix C**

# The Brant Haldimand Norfolk Catholic District School Board

Video Security Surveillance System

## STORAGE DEVICE RELEASE FORM

| | | | |
|---|---|---|---|
| **Date:** | **Time:** | **Storage Device ID#:** | **Form #:** |
| **Name of School/ Facility** | **Location of Storage Device**<br><br>□ In-Use _____<br>□ Used _____ | **Type of Device**<br><br>□ Tape □ CD □ Disk<br><br>□ Other (Specify) _____ | |
| **Name of Authorized BHNCDSB Individual Releasing Storage Device**<br><br>_____<br>Name (please print) | | **Signature** | |
| **Position** | **ID or Badge Number** | **Organization and Telephone Number** | |
| **Purpose or Reason for Release** | | | |
| **Disposition Following Use:** □ To be Returned to School/Facility of Origin<br>□ To be Destroyed<br>□ 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 --**

Audit Conducted (Date/Time): _____
Auditor's Name (Print Name): _____
Audit Organization (Print Name): _____
Signature of Lead Auditor: _____

**Appendix D**

# The Brant Haldimand Norfolk Catholic District School Board

Video Security Surveillance System

## STORAGE DEVICE DISPOSAL RECORD

| STORAGE DEVICE | | | DISPOSAL | | |
|---|---|---|---|---|---|
| **ID #** | **Type of Device (tape, CD, etc.)** | **Location In-Use or Used** | **Method of Disposal** / **Reason** | **Date & Time of Disposal** | **Signature** / **Name (Print)** |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Not Applicable for the Routine Over-Write/Erasure of Unviewed Recorded Material**

School or Faculty _____ Page _____ of _____

Audit Conducted (Date/Time): _____

Auditor's Name (Print Name): _____

Audit Organization (Print Name): _____

Signature of Lead Auditor: _____