HURON-PERTH CATHOLIC
District School Board

Video Surveillance Systems

Adopted:	**August 27, 2007**	**Policy #:**	**P 3.1.5.**
Revised:	**May 25, 2021**	**Policy Category:**	**3.1. Plant/Facilities**

POLICY STATEMENT:

The Huron-Perth Catholic District School Board ("HPCDSB" or the "Board") is committed to maintaining safe and orderly Christ-centered learning environments. This is accomplished primarily through teaching, modeling, and encouraging mutually-respectful relationships. Video surveillance systems are an additional resource used at schools within the Board's jurisdiction to further promote the safety and security of students, staff and community members and prevent destruction of school property.

Video surveillance involves the collection, retention, use and disclosure of personal information. Under the authority of the Director of Education, the principal or designated vice-principal will maintain control of and responsibility for the video surveillance system at all times. This Policy regulates the use of video surveillance systems by HPCDSB in accordance with *the Municipal Freedom of Information and Protection of Privacy Act* ("MFIPPA") and its associated regulations and Information and Privacy Commissioner of Ontario ("IPC") guidance.

This Policy is not intended to address or apply to:

- Instances where school videotape a specific event (such as a school fun fair or graduation ceremony); or
- Instances where a classroom is videotaped for educational or research purposes.

PROCEDURES:

1. Installation and Placement of Video Surveillance Equipment

1.1 Proper Purposes for Collection

1.1.1 Video surveillance systems should only be installed where video surveillance has been determined to be necessary for one of the following purposes:

1.1.1.1 Enhancing the safety of students, staff and community members;
1.1.1.2 Protecting school assets and property; and
1.1.1.3 Deterring and detecting criminal activity and vandalism.

1.2 Consultations before the Installation of Video Surveillance Systems at a New Location.

1.2.1 Before video surveillance takes effect in any location under the Board's jurisdiction, the following communication procedures will be carried out:

1.2.1.1 Consultation with School Council will occur;

1.2.1.2 The principal will issue an explanatory newsletter to parents and guardians;
1.2.1.3 The principal or vice principal will explain their use to all staff members and to students in class or grade-level meetings.

1.2.2 Approval for video surveillance shall be granted by the school's superintendent.

1.3 Design, Installation and Operation of Video Surveillance Equipment

1.3.1 In designing, installing and operating a video surveillance system, consideration shall be given to the following:

1.3.1.1 Reception equipment will only be installed in and monitor specified public areas, approved by the school's superintendent, where video surveillance is necessary to increase the safety of staff, students and/or school property. The equipment will operate up to twenty-four hours/seven days a week, within the limitations of system capabilities, power disruptions and serviceability/maintenance.
1.3.1.2 Equipment will not be installed in areas where the students, staff and the public have a higher expectation of privacy (e.g. change rooms and washrooms).
1.3.1.3 Reception equipment will be accessible only by authorized personnel (the principal or designate).

1.3.2 At all times, the Board maintains control of, and responsibility for, the video surveillance system and data produced.

2. **Signage and Notification**

2.1 Signs/notices will be posted at main entrances to the areas under surveillance to indicate the presence of video surveillance systems. Such signs will accord with the requirements of MFIPPA.

2.2 Explanatory notification will be included in the student handbook.

3. Disclosure, Retention, Security and Disposal of Video Surveillance Records

3.1 Lawful use of Personal Information.

3.1.1 As a general rule, the Board shall only use personal information collected by means of a video surveillance system for the purpose of the video surveillance program or for a consistent purpose, as set out at 1.1.

3.1.2 Video surveillance systems will not be used for the purpose of routine monitoring of employee performance and productivity, or to monitor student attendance.

3.2 Disclosure of Personal Information

3.2.1 The Board shall only disclose images captured by the video surveillance system in the circumstances permitted or required by MFIPPA.

3.2.2 The Board may disclose personal information to a law enforcement agency in the following circumstances:

3.2.2.1 Where the law enforcement agency approaches the Board, without a warrant, and requests that the Board disclose the records to aid an investigation from which a proceeding is likely to result. In such circumstances, the law enforcement agency must make a request for specific information in the context of a specific law enforcement investigation;

3.2.2.2 Where the law enforcement agency approaches the Board with a warrant or court order requiring the disclosure of the records; or

3.2.2.3 On the Board's initiative, where the Board has a reasonable basis to believe an offence has occurred. In this circumstance, the Board will only disclose the information that appears to be relevant and necessary for a potential investigation.

3.2.3 Before disclosing a storage device to a law enforcement agency, the Storage Device Release Log (Appendix A) will be completed. This form will indicate who took the device, under what authority, when this occurred, and if it will be returned or destroyed after use.

3.3 Retention, Storage and Destruction of Personal Information.

3.3.1 Records that have not been requested by law enforcement agencies or as part of an access request, or otherwise used or disclosed shall be retained for thirty (30) calendar days.

3.3.2 The retention period for recorded information which has been requested by law enforcement agencies or as part of an access request, or otherwise used or disclosed shall be a minimum of one (1) year. Records subject to this retention period will be transferred to removable media, appropriately labeled and stored in a secure location with controlled access.

3.3.3 The school will store and retain video files required for evidentiary purposes until the law enforcement authorities request them.

3.4 Protection of Records

3.4.1 The Board will employ physical measures to safeguard recorded data, including but not limited to:

- Storing physical records of footage, such as discs, memory cards or servers in a locked facility;
- Storing monitors in a secure location where they are not visible to the public.

3.4.2 The Board will employ administrative measures to safeguard recorded data, including but not limited to:

- Limiting access to recorded data to authorized personnel on a need-to-know basis;

- Granting accounts, systems, applications and devices only the degree and kind of access necessary to fulfill defined duties and functions;
- Keeping auditable logs of all accesses, uses and disclosures of footage that are generated automatically where records are maintained electronically;
- Whitelisting applications to help prevent malware and other non-approved programs from running;
- Using standard, secure system configurations and not using default or factory settings;
- Periodic maintenance of video surveillance systems will be performed by staff based on a schedule that will ensure efficient operation to the system.

3.4.3 The Board will employ technological measures to safeguard recorded data, including but not limited to:
- Strongly encrypting video surveillance footage at rest and when transmitted across open, public networks;
- Regularly patching systems and application to protect against vulnerabilities.

3.4.4 Vendors and/or service providers of HPCDSB's video surveillance systems shall not have access to recorded information without special permission. 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.

3.5 Disposal of Personal Information.

3.5.1 Once the retention period has expired for records, those media files 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.

4. Access and Correction of Personal Information

4.1 An individual whose personal information has been collected by a video surveillance system has the right of access to his or her personal information under section 36 of the MFIPPA unless an exemption applies under Section 38 of said *Act.*

4.2 The procedure for requesting one's own personal information is the same as the general access procedure found under the 3A:17 Freedom of Information and Protection of Privacy policy. This procedure is engaged by making a written request to the Director of Education

5. Training

5.1 The school's superintendent will ensure that the procedures of this policy will be addressed through a training session to principals whose schools will implement video surveillance systems. Principals will ensure that training which addresses staff obligations shall be conducted as necessary, both initially and on an ongoing basis.

6. Covert Surveillance

6.1 Prior to the use of covert surveillance, the individual(s) intending to use the covert surveillance must present an application to the school's superintendent for approval.

6.2 Upon approval from the school's superintendent, covert surveillance applications must be directed to the Director of Education for approval.

6.3 In coming to a determination as to whether to approve the application for covert surveillance, the decision-maker at 6.1 and 6.2 must consider whether:

6.3.1 There is a substantial problem that the covert surveillance is seeking to address;
6.3.2 There is a "strong probability" that surveillance will assist in solving that problem;
6.3.3 There are any other alternatives that could similarly address the substantial problem;
6.3.4 The benefits derived from the personal information acquired through the covert surveillance far outweighs the infringement on the privacy of the individual(s) being surveilled.

6.4 The covert surveillance must be time limited and case specific.

6.5 The reception equipment will be removed as soon as the case has been resolved or converted into overt surveillance in accordance with this Policy.

7. Evaluating the Use of a Video Surveillance System

7.1 The school's superintendent will conduct periodic and/or regularly review and evaluate the roles, responsibilities and practices of the Board's video surveillance programs to ensure they comply with this Policy, and applicable laws, regulations and policies.

7.2 If the school's superintendent identifies any deficiencies or concerns while conducting a review under 6.1, they will be addressed in a timely fashion.

7.3 Staff with access to the video surveillance system will be informed that their job activities may be subject to auditing, and that they may be called upon to justify particular instances where they accessed footage.

7.4 In addition, the school's superintendent will regularly review and evaluate the video surveillance procedure to ascertain whether it is still justified.

8. Respond

8.1 Upon discovering a privacy incident, staff will, as soon as reasonably possible, report the circumstances to the schools' superintendent.

8.2 Where a user has violated the Policy, they may be subject to discipline, up to and including termination.

DEFINITIONS:

Personal information: Defined by MFIPPA as recorded information about an identifiable individual, which includes, but is not limited to, information relating to an individual's race, colour, nationality or ethnic origin, sex, and age. If a video surveillance system displays these characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered "personal information".

Record: Defined by MFIPPA as any record of information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes but is not limited to a photograph, film, microfilm, videotape, digital recording, machine-readable record, and any record that is capable of being produced from a machine-readable record.

Video Surveillance System: Defined as 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 on Board property. The IPC includes in the term video surveillance system an audio device, thermal imaging technology, or any other component associated with capturing the image of an individual. This includes Reception Equipment.

Reception Equipment: Defined as equipment or device(s) 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: Defined as a videotape, digital video recorder, computer disk or drive, CD ROM, DVD, computer chip or other device used to store the recorded data or visual, audio or other images captured by a video surveillance system.

Privacy Incident: Defined as an incident where personal information may have been collected, retained, used, disclosed or disposed of in ways that do not comply with personal information protection requirements in statute, regulation and/or the Board's policies and procedures.

Covert Surveillance: Means systems are unnoticeable or hidden.

REFERENCES:

- N/A

RESOURCES, APPENDICES AND FORMS:

- N/A