Waterloo Catholic District School Board

Administrative Procedures Memorandum

#: APC028

Video Surveillance

Date of Issue: May 2004
Reviewed/Revised: February 2019

Memo To: All Staff and Stakeholders

From: Director of Education

ACCESSIBILITY:

To request this file in large print, please email aoda@wcdsb.ca or call (519) 578-3660.

PURPOSE:

Waterloo Catholic District School Board's video surveillance procedure has been modelled on the Guidelines for the Use of Video Surveillance by the Information and Privacy Commissioner of Ontario.

Video surveillance involves the collection, retention, use, disclosure and disposal of personal information. These activities must comply with the Municipal Freedom of Information and Protection of Privacy Act.

Video security surveillance systems are one resource used by the Board at selected schools/sites and on selected Board provided transportation services to promote the safety of students and staff.

REFERENCES:

- Education Act S265(1),S170(1), s11(3) of Reg. 298
- Municipal Freedom of Information and Protection of Privacy Act
- IPC Guidelines for the Use of Video Surveillance
- School Board - Police Protocol
- Student Transportation Services of Waterloo Region, Video Camera on School Purpose Vehicle Procedure

FORMS:

- APC028-01F: Video Surveillance Request (Online Form)

REPORTS:

- N/A

APPENDICES:

- N/A

COMMENTS AND GUIDELINES:

Definitions

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

2. **Record**: any record of information, however recorded, whether 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.

3. **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 on Board property.

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. **Storage Device**: a videotape, computer disk or drive, CD ROM, encrypted USB memory keys, computer chip or other device used to store the recorded data or visual, audio or other images captured by a video surveillance system.

Responsibilities

1. **Director of Education** is accountable for the overall Board video security surveillance program.

2. **Chief Information Officer** is responsible for the development and review of the policy and supporting guidelines along with the technical aspects of the video security surveillance systems.

3. **Privacy & Information Management Officer** (reporting to the Chief Information Officer) is the staff member responsible for the Board's privacy obligations under the Acts and the policy.

4. **Information Technology** is responsible for end user machine installation and configuration, for logging support requests and for providing on site or remote technical support.

5. **Senior Manager of Facility Services** is 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 training at Board sites. Facility Services is responsible for costs incurred for repairs, preventative maintenance, upgrades to video surveillance systems. Facility Services is also responsible for the coordination of equipment audits.

6. **Principal or Designate** of a school/site having a video security surveillance system is responsible for safeguarding personal information, and for the day-to-day operation of the system (e.g. validating cameras are working daily) in accordance with legislation, regulations, policies, guidelines. Other tasks include completing the Video Surveillance Request (Online Form APC028-01F) and adhering to direction/guidance that may be issued from time to time. Principal is also responsible for student behaviour concerns on Board-provided transportation.

7. **Student Transportation Services Waterloo Region (STSWR) Manager** is responsible for ensuring contracted transportation providers have video surveillance equipment installed on selected transportation vehicles and for ensuring that data sharing agreements are in place with all Board contracted transportation vendors. STSWR Manager may conduct investigations where there is a known concern/issue.

8. **WCDSB Internal Auditor** is responsible for conducting biannual audits.

Use of Video Security Surveillance System

1. Video surveillance footage remains the property of the Board.

2. WCDSB uses video security surveillance systems at selected schools, sites and on Board provided transportation services to promote the safety of pupils, staff and for the protection of Board and school sites against theft and vandalism. 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.

3. The Board will maintain control of, and responsibility for, the video surveillance footage at all times. Data sharing agreements must be in place between STSWR and contracted transportation service providers which 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.

4. STSWR contracted transportation service providers and their employees 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 selected transportation vehicles.

5. Further, the agreement between the Board and contracted service providers shall outline the use, collection, security, retention and disposition of all recorded information in accordance with this procedure.

Procedures for the Collection of Recorded Information

- 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 student, staff and public safety or to detect and deter criminal activity and vandalism.

- The equipment shall be installed in such a way that it only monitors those spaces that have been identified as requiring video surveillance and shall not be directed beyond school/board property. Cameras should not be directed to look through the windows of adjacent buildings.

- Only the school principal, or designate, the Manager of STSWR or, designated IT or Facility Services staff may review recorded information. Circumstances where review may be warranted will normally be limited to further investigation of an incident that has been reported/observed or to investigate a potential crime.

Security Measures for Video Surveillance Information

1. Ensure the safe guarding, confidentiality, integrity and availability of footage captured by the system

2. Encrypt at rest and when transmitted across public networks

3. Secure footage in a locked facility

4. Limit staff and other individuals access to footage ("need to know basis"). See Responsibilities

5. Store monitors in a secure location not visible to the public

6. Limit account access to video surveillance systems and applications only when required

Access and Disclosure of Recorded Video Surveillance Information

1. All recorded images are the property of the Board and shall be used, disclosed, retained, secured and disposed of in accordance with the Municipal Freedom of Information and Protection of Privacy Act.

2. 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 the Municipal Freedom of Information and Protection of Privacy Act. This request can be made through an official Freedom of Information Request. Access to an individual's own personal information in these circumstances may also depend upon whether any exemptions apply and if the information can be reasonably severed from the record.

3. Third parties external to the Board must file a Freedom of Information Request prior to being granted any access to this information.

4. The only exception is law enforcement when they are conducting an investigation on our behalf.

5. If the police are requesting information/video surveillance footage not related to a school investigation, it must be done through a warrant process.

6. If information has been viewed and deemed relevant for a law enforcement or school/bus safety investigation, the relevant information must be extracted and secured by the school principal or designate, manager of STSWR. or relevant senior Board Officer.

7. Each school/site including STSWR that has a video surveillance program in place must ensure there is an audit trail of requests. Schools must complete the Video Surveillance Request (Online Form APC028-01F). STSWR must retain its own log book. The log should indicate who took the footage, under what authority, request date, time of day the event took place, a description of the circumstances justifying disclosure and if it will be returned or destroyed after use.

8. When disclosing video footage, ensure the extracted video is in Bosch native file format.

9. If you have any questions pertaining to the disclosure/release of this information or any inadvertent disclosure, please contact the Privacy and Information Management Office.

Procedures for the Retention of the Recorded Information

- The retention period for information that **has not been viewed** for law enforcement, school or safety purposes shall be a maximum of 30 calendar days.

- 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, schools must retain the section of footage viewed for one year. If, however, the information has been placed on legal hold, then the information must not be destroyed until further notice.

- Destroy old storage devices in such a way that the personal information cannot be reconstructed or retrieved. Maintain a record of the disposal date in a log.

Auditing and Evaluating the Use of a Video Surveillance System

1. The Board will ensure that the use and security of video surveillance equipment is subject to regular audits.

2. The audit will address the Board's compliance with the appropriate legislation and Board operational policies.

3. The Board will immediately address any deficiencies or concerns identified by the audit.

4. Employees with authorized access to video surveillance equipment and service providers must 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.

5. Audits will include but are not limited to the following areas:

    - Equipment function
    - Area being captured by surveillance equipment
    - Records retention
    - Notification signage