

## VIDEO SURVEILLANCE – FACILITIES AND SCHOOL BUSES

### Background

The Division recognizes its responsibility for and the importance of providing a safe, healthy environment for students and staff while on Division property. Video monitoring, and consequently its audio recording, in some cases, may be used on school property, including school buses, to monitor the safety and security of individuals and property in accordance with these procedures.

### Definitions

Other than Titles or Sub-titles, when terms appear in **bold-face** type please refer to the definition section for improved understanding of the term.

**Access:** is a person's ability to view or copy **records**

**Authorized employee:** are those employees who are required to collect, **access**, use, store, retain, disclose or dispose of **personal information** in the execution of their work-related duties, on a need to know basis, for the purpose of this administrative procedure.

**Personal Information:** Section 1(n) of the *Freedom of Information and Protection of Privacy* (FOIP) Act - recorded information about an identifiable individual, including:

- An individual's name, home or business address, or home or business telephone number,
- The individual's race, national or ethnic origin, colour or religious or political beliefs or associations,
- The individual's finger prints, other biometric information, blood type, genetic information or inheritable characteristics,
- Information about the individual's health and health care history, including information about a physical or mental disability,
- Information about the individual's educational, financial, employment or criminal history, including criminal **records** where a pardon has been given,
- Anyone else's opinions about the individual, and
- The individual's personal views or opinions, except if they are about someone else

**Record:** A record is information in any form and can include notes, images, audiovisual recordings, emails, text messages, drawings, photographs and any other information that is written, photographed, recorded or stored in any manner.

**Surveillance:** refers to a mechanical or electronic system or device that enables continued or periodic video recording, observing or monitoring of personal information about individuals in open, public spaces, public buildings or public transportation, including school and municipal transit buses or other similar vehicles.

## **Procedures**

1. Notification shall be displayed when any monitoring system is active.
  - 1.1. Signs shall be posted advising of the area of the presence of video monitoring.
  - 1.2. Students, parents/legal guardians and staff will be informed at the beginning of the school year, or at any other point, as required, that the Division will be monitoring all activity which occurs at designated monitoring points, and video/audio **surveillance** may be used by the Division as evidence.
    - 1.2.1. Notification may be done through email, newsletter and/or in person.
2. Location and Control
  - 2.1. Division sites and contracted school buses, may be equipped with video monitoring devices. The installation of these devices must be approved by the Secretary Treasurer.
  - 2.2. Video **surveillance** may only be placed:
    - 2.2.1. In areas where it is necessary to assist in ensuring the personal safety of individuals and/or to monitor activity.
    - 2.2.2. In areas where student supervision is difficult
    - 2.2.3. In areas where monitoring has proven to be necessary as a result of prior property damages or related security incidents;
    - 2.2.4. In areas where the video monitoring will be deemed to be a viable deterrent;
  - 2.3. Video cameras will not be used to monitor areas where the public has a reasonable expectation of privacy, including change rooms and washrooms;
  - 2.4. Cameras shall not be directed to look through windows of adjacent non-division buildings.
  - 2.5. The Principal, Site Supervisor, or other **authorized employee** is responsible to audit the use and security of **surveillance** equipment, and report utilization to the

Secretary Treasurer.

### 3. **Access** and Use

- 3.1. **Access** to the video/audio information collected can only be **authorized** by the FOIP Coordinator (Secretary Treasurer), or designate.
- 3.2. Video/audio recordings of actions by student(s) or staff may be used as evidence in any disciplinary action brought against an individual arising from conduct on or around Division property or with regard to student transportation.
- 3.3. Recordings may be used to detect or deter criminal offences, when requested by law enforcement.
- 3.4. Video/audio recordings may be released to third parties or applicants in conformance with the provisions contained in the FOIP, and any rules or regulations thereunder.
- 3.5. The Division shall not use video/audio recordings for other purposes unless expressly authorized by or under an Act or enactment and will only use video/audio recordings in such a manner as to avoid public viewing.
- 3.6. **Surveillance** will only be used where conventional means for achieving the same objectives are substantially less effective than **surveillance** and the benefits of **surveillance** substantially outweigh any reduction of privacy in the existence and use of the system.

### 4. Protection of Information, Disclosure, Retention, and Disposal

- 4.1. All video/audio recordings shall be securely stored in a locked area at the respective Division site and viewed only through **authorized access**.
- 4.2. The Secretary Treasurer is responsible for enforcement of video/audio monitoring and must authorize **access** to all recording devices or video/audio **records**.
  - 4.2.1. A log shall be maintained of all **access** to, or use of recorded material.
  - 4.2.2. The Secretary Treasurer shall ensure that a Law Enforcement Disclosure form AP 170 (Appendix D), a Storage Device Release form (Appendix A), or a Request for Information form AP 170 (Appendix C) is completed before disclosing recordings or recording devices to appropriate authorities or third parties. Any such disclosure shall only be made in accordance with applicable legislation.
  - 4.2.3. An individual, or a parent/guardian of an individual, who is the subject of video **surveillance** has the right to request **access** to the recording in the presence of the FOIP Coordinator (Secretary Treasurer) or **authorized employee** and in accordance with FOIP.

4.2.3.1. Viewing may be refused or limited where it is deemed that it would be an invasion of a third party's personal privacy, would give rise to a concern for a third party's safety, or any other grounds recognized in the FOIP Act.

4.3. Any **record** created as a result of video/audio monitoring will be retained and destroyed according to the Division Records Retention Schedule. All **records** containing **personal information** which has been used to make a decision that directly affects an individual shall be retained for a minimum of one (1) year. All other **records** shall be retained for thirty (30) days.

4.3.1. All recordings shall be disposed of in a secure manner.

4.4. Any actual or suspected privacy breach of the FOIP Act (see AP 170), whether intentional or not, must be reported to the FOIP Coordinator immediately.

4.4.1. The Division will not take any adverse employment action against a Division employee who, acting in good faith, reported an actual or suspected breach of the FOIP Act (see AP 170) by another Division employee to the FOIP Coordinator.

4.5. The Division employee who contravenes the FOIP Act (see AP 170) or this Administrative Procedure may be subject to disciplinary action up to and including termination or employment or contract with the Division.

4.6. Video monitors are to be in a controlled **employee access** area wherever possible.

## 5. Non-application

5.1. These procedures do not apply to covert or overt **surveillance** cameras being used by or on behalf of the Division as a case specific investigation tool for law enforcement purposes, where there is statutory authority and/or authority of a search warrant to conduct the **surveillance**.

### Reference:

- [Education Act](#)
- [Freedom of Information and Protection of Privacy Act](#)
- [Freedom of Information and Protection of Privacy Regulation](#)
- [Administrative Procedure 170 – Freedom of Information and Protection of Privacy](#)

Implementation Date: February 19, 2020

**STORAGE DEVICE RELEASE FORM**  
**Request for Disclosure under the**  
***Freedom of Information and Protection of Privacy Act***

Date

In accordance with the *Freedom of Information and Protection of Privacy Act*, the

\_\_\_\_\_ (name of public body)

requests disclosure the surveillance storage device located at:

\_\_\_\_\_ (name of location)

Will the requested storage device be returned to Greater St. Albert Catholic Schools or destroyed by the requesting public body, after use?

\_\_\_\_\_ (returned or destroyed)

This information is required by this public body to assist in an investigation pursuant to:

\_\_\_\_\_ (reference to a federal or provincial statute or description of purpose)

**Requesting Official**

\_\_\_\_\_ Name

\_\_\_\_\_ Title

\_\_\_\_\_ Signature

\_\_\_\_\_ Badge Number (if applicable)

**THE BELOW INFORMATION IS TO BE FILLED OUT BY GREATER ST. ALBERT CATHOLIC SCHOOLS, SECRETARY TREASURER**

I, hereby,  Consent  Refuse this disclosure of personal information to:

\_\_\_\_\_ (name of public body)

**Greater St. Albert Catholic Schools Authorized Disclosing Official**

Secretary Treasurer

\_\_\_\_\_ Name

\_\_\_\_\_ Title

\_\_\_\_\_ Signature

Greater St. Albert Roman Catholic Separate School Division

\_\_\_\_\_ Name of Public Body

**NOTE: This completed record may qualify for exception to disclosure under section 20 of the *Freedom of Information and Protection of Privacy Act*.**