Rationale

For reasons of enhancing the safety of students, staff and others on school premises and deterring destructive acts, the CISPG Board authorizes the use of video surveillance equipment on School property where circumstances have shown that it is necessary for these purposes and its benefit outweighs its impact on the privacy of those observed.

The Board recognizes both its legal obligations to provide appropriate levels of supervision in the interests of student safety and the fact that students and staff have privacy rights that are reduced, but not eliminated, while at school. Thus, video surveillance must be carried out in a way that respects student and staff privacy rights.

A recording is recognized to be subject to the provisions of the Personal Information Privacy Act (PIPA) of which CISPG Schools adhere.

Policy

CISPG schools may purchase, install and use video surveillance equipment on school property. The church may have its own cameras and monitors and is bound by their own diocesan policy on video surveillance. Given that the school and church are on the same property, they may have a joint plan that is submitted to the Bishop and Superintendent by the Pastor (in consultation with parish council) and Principal (in consultation with school council). In such cases, both the pastor and principal have the same status as supervisors in this policy. All authorized persons should have necessary training to understand privacy and security obligations under PIPA.

Procedures

1. Use

    a. Installation of video surveillance equipment must be done in accordance with the guidance document from the Office of the Information and Privacy Commissioner for British Columbia *Using Overt Video Surveillance* (October 2017).

    b. Video surveillance camera locations must be jointly authorized by the principal and school council. The principal and school council submit a joint plan/report to the Superintendent for review and approval. The report should describe the circumstances that indicate the necessity of having surveillance at that site, including less invasive alternatives considered. It should include the placements for the installation of the cameras and where the monitor(s) will be. Any change in camera location must be authorized in the same manner. The contractor who installs the system must be certified for such installations and approved by the principal.

c. Public notification signs, clearly written and prominently displayed, must be in place in areas that are subject to video surveillance. Notice must include contact information of the principal or designated staff person who is responsible for answering questions about the surveillance system. Any exception to this, such as for a time-limited specific investigation into criminal conduct, must be authorized by the Superintendent on the grounds that covert surveillance is essential to the success of the investigation and the need outweighs the privacy interest of the persons likely to be observed. Covert surveillance may not be authorized on an ongoing basis.

d. Video surveillance is not to be ordinarily used in locations where appropriate confidential or private activities/functions are routinely carried out (e.g. bathrooms, changerooms, private conference/meeting rooms or offices). The Superintendent must authorize any exception to this on the grounds that no other supervision option is feasible and that the need is pressing and outweighs the privacy interest of the student or other person likely to be observed. Surveillance of such locations may not be authorized on an ongoing basis.

e. If video surveillance is already installed, a school must demonstrate that the system is in compliance with this policy. Should the current system not be in compliance with this policy, the Principal will enact a plan to bring it into compliance within a reasonable time, approved by the Superintendent.

2. Security

a. A contractor approved by the principal must be employed to install video camera equipment. The principal or his/her designate of the school and the Superintendent shall have access to the cameras and footage.

b. Video files shall be stored in a secure/locked area to which students and the public do not normally have access, or in a locked area to which students and the public do not have access.

c. Files may never be sold, publicly viewed or distributed in any other fashion except as provided for by this policy and appropriate legislation.

3. Inadvertent privacy breach resolution process

a. Should an inadvertent disclosure of private information occur, the first step is to contain the breach to ensure that additional disclosure is averted. This may require shutting down the video surveillance system until the matter is resolved. A record of the breach is to be noted in a disclosure log indicating whose privacy was breached, the date and time, how the disclosure occurred and the person(s) to whom the private information was inadvertently disclosed.

b. An assessment of the breach must be immediately conducted by the principal and, if applicable, the pastor. The assessment must seriously consider the potential damage to those affected by the breach. If there is more than a low risk of damage, those whose private information has been disclosed are to be notified in writing (including email)

within one business day of the discovery of the inadvertent disclosure including all of the information recorded in the disclosure log.

c. Any person affected by a breach must be permitted to view any of their private information that was disclosed in the privacy breach unless such information will create an additional privacy breach.

d. In some cases, where the breach is significant, additional reporting requirements may apply, up to and including disclosure to the Superintendent or designate, who will determine whether any additional action is required.

4. Viewing of Files

a. Video monitors used to view video files should not be located in a position that enables viewing except by the principal or their designate.

b. Video files may only be viewed by:

- the principal and/or Superintendent or their designate

- parents and students - parents or guardians requesting to view a segment of a video file that includes their child/children may do so. Students may view segments of the file relating to themselves if they are capable of exercising their own access to information rights under the *Privacy Information Protection Act.* Student/ parent/guardian viewing must be done in the presence of the principal. Viewing may be refused or limited where viewing would be an unreasonable invasion of a third party's personal privacy, would give rise to a concern for a third party's safety, or on any other ground recognized in the *Personal Information Privacy Act*.

- employees or contractors responsible for the technical operations of the system (for technical purposes only)

- law enforcement agencies at the discretion of the principal. Incoming requests for recordings or viewings from other public bodies or law enforcement agencies must be justified and must contain the following information:

    - The name of the individual whose information is requested.
    - The precise nature of the information requested.
    - The authority for the investigation.
    - The purpose for which the requesting public body will use the information.
    - The name, title and address of the person authorized to make the request.
    - If pursuant to a court order, a copy of the order.

5. Retention of Video Files

a. Where an incident raises a prospect of a legal claim against the School, the file, or a copy of it, shall be sent to the School Board's insurers.

b. Video files shall be erased within one month unless they are being retained at the request of the principal, Superintendent, employee, parent or student for documentation related to a specific incident or are being transferred to the Board's insurers.

c. Files retained under section 5a shall be erased as soon as the incident in question has been resolved, except that if the file has been used in the making of a decision about an individual, the file must be kept for a minimum of one year as required by the *Personal Information Privacy Act* unless earlier erasure is authorized by or on behalf of the individual.

6. Review

a. The principal is responsible for the proper implementation and control of the video surveillance system.

b. The Superintendent of Schools or designate may conduct a review at any time to ensure that this policy and these procedures are being adhered to.

Resources

Public Sector Surveillance Guidelines, updated January, 2014 - Office of the Information and Privacy Commissioner for British Columbia - Province of BC

Guide to Overt Video Surveillance, October 2017
Office of the Information & Privacy Commissioner for British Columbia

References:	***Date:*** June 2024
	Revisions: