#1113593 ECAE

Video Surveillance

This regulation has been created in accordance with the Freedom of Information and Protection of Privacy Act (FIPPA), and the Video Surveillance Guidelines in public spaces as issued by the Manitoba Ombudsman.

1. Guidelines for use of Video Surveillance

- Video surveillance will only be used where it is deemed necessary for the purposes of enhancing safety of persons, or for the deterrence and protection from theft or destructive acts, and/or property damage such as vandalism and graffiti.
- Video surveillance must be conducted in accordance with the laws of Manitoba and Canada.
- Video surveillance will only be used where it is deemed necessary for the purposes of enhancing safety of persons, or for the deterrence of theft or destructive acts, such as vandalism and graffiti.
- Appropriate signs and notice of video surveillance must be posted in areas subject to video monitoring.
- Staff and video service providers (third-party), will have access to information collected through video surveillance only where necessary in the performance of their duties and in accordance with the provisions of this policy.
- Staff and video service providers (third-party) who may require access to information collected through video surveillance will be provided proper training and orientation with regards to this policy and their obligations under this policy and the Act, and will provide written acknowledgment that they have read and understood the contents of this policy and procedure. Any staff who knowingly or deliberately breaches this policy or the Act will be subject to discipline up to and including termination. Failure of a video service provider to comply with this policy or the Act will constitute breach of contract and may result in termination of contract and legal action.
- To monitor and deter criminal activity from occurring.
- Real time monitoring may be used for the purpose of identifying problems that require immediate intervention and for the safety of people on the premises during regular school hours, after hours and weekends to monitor community use of schools.
- Real time monitoring may be used for other purposes such as monitoring weather conditions for grounds maintenance purposes (e.g. ice and snow removal).

2. Design and implementation of a surveillance system

- All cameras must be unconcealed and clearly visible.
- Cameras shall not be placed in change rooms, washrooms and areas where students, staff and others have a reasonable expectation of privacy.
- Cameras located internally shall not be directed to look through windows to areas outside the building, unless necessary to protect external assets, provide for the personal safety of individuals on school premises, or to deter criminal activity from occurring.
- Any change in camera location, or additional camera installations must be authorized by the Superintendent/Chief Executive Officer or designate.

3. Notifying the public

- Signs advising use of the presence of video surveillance practices should notify individuals of:
    a. The area in which surveillance is conducted.
    b. The purpose for the surveillance.
    c. Hours during which surveillance is conducted.
    d. Who is responsible for conducting surveillance in the department; and
    e. The contact person responsible for answering questions about the cameras; including an address or telephone number for contact purposes.
- All staff and contractors shall be advised of this policy.

4. Using and disclosing surveillance records

Use of Recorded Information

The school principal or his or her designate may use recorded information for purposes as outlined in this policy and for the purposes expressly stated by or under the Act.

Access to Recorded Information

- Only the school principal or his or her designate, and members of the Winnipeg Police Service shall have access to the electronic surveillance system while it is in operation.
- The school principal and/or his or her designate must authorize access to all recorded information.
- Recorded information must be viewed in such a manner as to avoid public (covert) viewing.

- Computer monitor and recording shall be password protected, encrypted and stored in a secure area away from public viewing and should be in a position that cannot be viewed by others.
- A log shall be maintained by school principal and/or his or her designate of all episodes of access to, and/or use of recorded information
- Parents and or guardians may review a segment of the recording if the segment relates to a specific incident (e.g. accident or misconduct) involving their child or children, unless this violates the privacy of a third party. In that case, the review should not take place unless authorized by the School Division Privacy Officer and in accordance to FIPPA. Students may be permitted access to view a segment of a recording relating to themselves if they are capable of exercising their own access to information rights under the FIPPA. Student, parent, guardian access to record viewing granted under FIPPA must be done in the presence of an administrator.

5. Retention and destruction of surveillance records

- All recorded information used to make a decision that directly affects an individual shall be retained for a minimum of one year; with the exception of information specifically awaiting review by law enforcement agencies, information seized as evidence, or information that has been duplicated for use by law enforcement agencies
- All recorded information shall be disposed of in a secure manner

6. Security of surveillance records

- All recorded information not in use shall be securely stored in a locked receptacle or area
- Recorded information may never be sold, publicly viewed or distributed in any other manner except as provided for by this policy and appropriate legislation
- All recorded information used for the purpose of this policy shall be numbered, electronically dated, and retained for 2 weeks during the school year, and up to 6 weeks during the summer break.

7. Access to surveillance records

- Recorded information may be disclosed to applicants in conformance with the provisions contained in the Access to Information and Protection of Privacy Act and in such other cases as required by law.
- The school principal or his or her designate shall ensure that a recorded information release form is completed before disclosing recorded

information to appropriate authorities or third parties. Any such disclosure shall only be made in accordance with applicable legislation.

- A recorded information release form should indicate the individual or organization who took the recorded information, the date of occurrence or when and if the recorded information will be returned or destroyed by the authority or individual after use.

8. Auditing surveillance systems

- The Divisional Supervisor, Accounting will be responsible to audit the use of security or surveillance cameras, including recorded information, and to ensure that this policy and procedures are being adhered to and to make an annual report to the Senior Administration on any findings.

9. Leased or Rent to a Tenant

- This policy does not apply to Division owned property that is being leased or rented to a tenant. Private-sector organizations in Manitoba should refer to *Personal Information Protection and Electronic Act* (PIPEDA) for reference.
- A tenant who leases or rents Division owned property may not place any exterior cameras and/or in areas of shared space for their purpose without consulting the Superintendent/Chief Executive Officer or designate.