1. GENERAL

1.1 The purpose of this policy is to create and maintain a safe school and work environment for students, staff, parents and members of the community. Security cameras (closed circuit television systems – CCTV) are installed in schools to monitor school property, to assist school administrators in detecting and deterring unacceptable behaviour or activities, and to assist in investigations, when required. Security cameras may be installed in other non-school buildings and on Division properties, including school buses.

1.2 This policy does not apply to covert surveillance or surveillance when used as a case-specific investigation tool for law enforcement purposes where there is statutory authority and/or the authority for a search warrant to conduct the surveillance.

1.3 This policy will apply to situations where permanent video surveillance cameras have been placed on school division property including school buses. This policy is not intended to deal with instances where school officials videotape a specific event such as a performance or graduation ceremony, or an isolated instance where a classroom is videotaped for education or research purposes.

1.4 This policy will ensure that the Winnipeg School Division (WSD) meets its obligations under The Freedom of Information and Protection of Privacy Act (FIPPA) and The Personal Health Information Act (PHIA), and other applicable legislation, including WSD Policies.

1.5 School divisions are required to comply with FIPPA and PHIA legislation, which governs access to and protection of personal information or personal health information, and addresses the collection, use, disclosure, security and independent review process relating to personal information.

1.6 The collection, use, protection, retention and/or disclosure of information shall be in accordance with the provisions of the Freedom of Information and Protection of Personal Privacy Act (FIPPA), the Personal Health Information Act (PHIA), the Youth Criminal Justice Act as well as Policy EGC – Records Management and Retention.

1.7 All employees are required to immediately notify either the Access and Privacy Officer and/or Access and Privacy Coordinator if a breach in privacy has occurred in order to contain the breach.

1.8 Should any WSD Policy conflict with FIPPA or PHIA legislation, the provisions of FIPPA or PHIA shall prevail unless otherwise expressly provided for by other applicable law.

2. POLICY DEFINITIONS

The following terms have the following defined meanings for the purpose of this Policy:

2.1 CCTV means closed-circuit television.

2.2 Personal Information means Recorded Information about an identifiable individual, as identified in part 1 of FIPPA.

2.3 Personal Health Information is Recorded Information about an identifiable individual as identified in part 1 of PHIA.

2.4 Persons Associated with the WSD means an employee, or agent who is associated with the WSD by appointment, employment, contract, or agreement.

2.5 Access to Information means the viewing or copying of a Record held in the custody or under the control of a public body or trustee.

2.6 Disclosure of personal information and personal health information means making the information known, revealing, exposing, showing, providing, selling or sharing the information with any person or entity outside of the WSD. FIPPA and PHIA permit disclosures of Personal Information and Personal Health Information for authorized purposes only and within limitations.

2.7 Privacy Breach occurs when there is unauthorized collection, use, disclosure or destruction of personal or personal health information. Such activity is "unauthorized" if it occurs in contravention of FIPPA or PHIA e.g. when personal health information about students or employees is stolen, lost or mistakenly disclosed.

2.8 Record or Recorded Information means a Record of information in any form, including information that is written, photographed, recorded or stored in any manner, on any storage medium, or by any means, including by graphic, electronic or mechanical means, in the custody or under the control of the WSD.

2.9 Third Party, in relation to a request for access to a Record or for correction of Personal Information, means any person, group of persons or organization other than

(i) the person who made the request, or
(ii) a public body

3. AUTHORITY

3.1 In accordance with Section 80 of the Freedom of Information and Protection of Privacy Act, and By-law 1065, the Chief Financial Officer/Secretary-Treasurer has been designated as the Access and Privacy Officer and the Board & Community Liaison Officer has been designated as the Access and Privacy Coordinator for the WSD.

3.2 The collection of personal information using CCTV systems is set out in subsection 36(1) of the Freedom of Information and Protection of Privacy Act.

4. PURPOSE

4.1 This policy will abide by the provisions that govern notice, access, disclosure, retention, security and disposal of the personal information that is being collected, in accordance with the Freedom of Information and Protection of Privacy Act.

4.2 The WSD will use CCTV systems for the following purposes:

a) To enhance the safety of students and staff;
b) To protect school property against theft or vandalism;
c) To assist in the identification of intruders and of persons endangering the health, well being or safety of students, staff, parents and members of the community;
d) To assist law enforcement in the investigation of criminal activity.

5. NOTIFICATION OF USE OF VIDEO SURVEILLANCE

5.1 The WSD will ensure that students, parents, staff and the public are notified annually that video surveillance is being used to monitor public areas in schools, and non-school buildings, including school buses.

5.2 The WSD will further ensure that students, staff, parents and members of the public have reasonable and adequate warning that surveillance is, or may be, in operation by using signs or posters prominently at the perimeter of the video security surveillance area, identifying video surveillance equipment locations.

5.3 The signage or posters must include the contact information for the Access and Privacy Coordinator as the person who can respond to questions regarding the collection of video surveillance footage. The WSD shall also ensure notification explains why surveillance is being conducted, at what times it is being conducted, the legal authority for surveillance and how individuals may make an access request to view their personal information which has been recorded.

6. COLLECTION OF VIDEO SURVEILLANCE FOOTAGE

6.1 The WSD may collect personal information for the purposes set out in subsection 36(1)(b) of FIPPA.

7. USE OF VIDEO SURVEILLANCE FOOTAGE

7.1 The WSD may only use video surveillance footage for the purpose for which the information was collected or compiled or as otherwise authorized in section 44 of FIPPA.

7.2 Video surveillance will not be used to monitor, audit or evaluate the job performance of employees for disciplinary purposes.

8. ACCESS TO VIDEO SURVEILLANCE INFORMATION

8.1 Access to General Information and Personal Information (Excluding Personal Health Information)

(a) FIPPA allows any individual a right of Access to Information held in the custody or under the control of public bodies, subject to specific exceptions. This includes access to general information held by the WSD, as well as Personal Information about the individual requesting the Record(s). Request forms may be found at www.gov.mb.ca/chc/fippa/appforms.html

(b) A formal Access to Information request is required if the information concerns:
(i) Confidential Information,
(ii) Personal Information concerning an individual employee/student, or
(iii) Third Party business information.

(c) A formal Access to Information request must be submitted to the Access and Privacy Coordinator, as described by Sections 8(2) and 8(3) of FIPPA. If the formal request is received by another department or school, it will be immediately forwarded to the Access and Privacy Coordinator. All formal requests will be reviewed by the Access and Privacy Coordinator.

8.2 The Chief Superintendent/designate, Access and Privacy Officer and/or Coordinator or Principal/Vice-Principal may disclose information in relation to a criminal investigation, including any surveillance camera recordings to the Winnipeg Police Service or other law enforcement agency as authorized in Section 44 (1)(r) of FIPPA.

8.3 All requests for information will require the WSD's Law Enforcement Disclosure form to be completed by the representative of the public body making the request. A copy of the completed form will be sent to and kept on file by the Access and Privacy Coordinator.

8.4 All other requests for access to information under FIPPA and PHIA and law enforcement requests not relating to criminal investigations shall be facilitated by the Access and Privacy Officer and/or Coordinator.

8.5 The Access and Privacy Officer and/or Coordinator may facilitate the viewing of recordings only for the purposes set out under this policy.

8.6 The videotaped evidence shall only be made available to those individuals or organizations who have a legitimate right to access the evidence.

8.7 Only that videotaped evidence which is necessary to identify the offender(s) and, where applicable, provide evidence for discipline or prosecution shall be retained and all other videotaped evidence shall be destroyed, subject to the retention periods that are set out in this policy.

8.8 Recordings may only be reviewed by the principal/vice-principal or staff member who has direct involvement with the contents of the specific recording.

8.9 Students may view a segment of a recording relating to themselves if they are capable of exercising their own access to information rights under FIPPA. Student/parent viewing must be done in private and in the presence of the principal or designate. An individual whose personal information has been collected and recorded by a video surveillance system may request access to the information in accordance with FIPPA. Records may be disclosed to law enforcement to assist in investigations as authorized by FIPPA.

Access requests to video surveillance records which may identify other individuals or their personal information may not be authorized under FIPPA or PHIA.

8.10 Only the principal or designate shall have access to a video surveillance storage device. The storage device shall be password protected and stored in a secure area.

9. INSTALLATION OF VIDEO SURVEILLANCE

9.1 The installation of video surveillance shall be conducted in accordance with the following:

- The placement of the cameras shall be such to minimize intrusion into the privacy of individuals who may be viewed by the cameras. Cameras should not be placed in areas which individuals have a heightened expectation of privacy, including inside and immediately outside washrooms and change rooms.

- The minimum number of cameras necessary to survey the area shall be used.

- The Director of Buildings will approve the location or relocation of cameras on WSD property. Cameras must not be relocated without permission from the Director of Buildings.

10. VIDEO SURVEILLANCE RECORDS

10.1 Video surveillance records will be in the custody of or under the control of the WSD and subject to FIPPA and/or PHIA legislation, as applicable.

10.2 Unless an investigation is underway, information obtained through video surveillance records will be deleted within 14 calendar days.

10.3 Video surveillance records accessed under a Freedom of Information and Protection of Privacy Act request shall be retained for a minimum of 45 calendar days after the records have been disclosed to the applicant to allow the applicant an opportunity to file a complaint with the Ombudsman and for such longer periods as may be prescribed for any appeal or statutory review thereof.

10.4 If decisions are made by the WSD based in whole or in part on information obtained through video surveillance, the information and video surveillance record(s) will be retained by the School Board for a minimum of one (1) year from the date the decision was made.

10.5 All information obtained through the use of video surveillance will be protected and handled in accordance with the requirements of the *FIPPA.*

11. LAW ENFORCEMENT

11.1 Video surveillance may be authorized for a limited time by the Chief Superintendent or designate, for specific investigation into complaints of criminal conduct or student misconduct 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.

11.2 Covert cameras will be left in place for only the period of time necessary to identify the offender(s) and obtain sufficient evidence for discipline or prosecution.

11.3 Temporary installations of video surveillance cameras for specific investigative purposes do not require the approval of the School Board and are exempt from the notification requirements of this policy.

12. RETENTION

12.1 Video surveillance footage shall be retained in accordance with the capability of the equipment, however, not longer than 14 days past the original recording date.

12.2 In determining what is a reasonable period of time the following factors shall be taken into consideration:

- the existing policy of the WSD entitled Policy EGC - Records Management and Retention; and
- the existing guidelines established by Manitoba Education *Guidelines on the Retention and Disposition of School Division/District Records*.

12.3 Subject to any longer retention period required by policy or applicable legislation, video Surveillance Records shall be erased, unless they are being retained at the request of the Principal/Vice-Principal, Chief Superintendent/designate or the Access and Privacy Officer/Coordinator, employee, parent or student for documentation related to a specific incident or are being transferred to the Boards' insurers and/or solicitors.

13. DESTRUCTION OF SURVEILLANCE FOOTAGE

13.1 In accordance with the Manitoba Education Guidelines on the Retention and Disposition of School Division/District Records, a log of records destroyed that meets the requirements of subsection 17(4) of PHIA must be kept for the destruction of records that contain personal health information. For all other records, school division/district policies and procedures should specify that a log of records destroyed be maintained. The log should include a description of the records, the date range and amount of records, and the date, method and person responsible for destruction as per the Destruction of Records form.

14. SECURITY SAFEGUARDS

14.1 All staff are responsible for the protection (security) of Personal Information and Personal Health Information:

a) Personal Information and Personal Health Information shall be protected by the WSD during its collection, access, use, disclosure, retention, storage, transportation, transmission, transfer and during its destruction.

b) All staff and people associated with the WSD are responsible for protecting Personal Information and Personal Health Information that is collected, heard, handled, viewed or processed in the discharge of their duties and responsibilities with the WSD.

c) All staff and people associated with the WSD who are dealing with Personal Information and Personal Health Information in any manner shall take all reasonable precautions to protect the Personal Information and Personal Health Information from fire, theft, vandalism, deterioration, accidental destruction or loss and any other hazards.

d) Reasonable administrative, technical and physical safeguards shall be taken by the WSD to ensure the confidentiality, integrity and security of Personal Information and Personal Health Information, and to prevent the unauthorized collection, access, use, disclosure, transport, transmission, transfer and destruction of Personal Information and Personal Health Information.

e) Personal Information and Personal Health Information stored in electronic form on a fixed computer server or terminal shall be properly secured from unauthorized access by reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the records.

14.2 The use and security of surveillance equipment, including cameras, monitors and storage devices, shall be annually audited by the Principal to measure compliance with this Policy.

14.3 Staff and contractors who have access to the surveillance system shall be provided periodic training concerning compliance with this Policy and applicable laws.

14.4 The Principal shall maintain an access log system which indicates when records were viewed or used, by whom and for what purpose, as well as information about which records were disclosed to Third Parties, to which Third Parties records were disclosed, when and for what purpose.

15. BREACH OF PRIVACY

15.1 A Breach of Privacy occurs when Personal Information, including Personal Health Information, is collected, accessed, used, disclosed, transported, transmitted, transferred or destroyed other than as authorized, or when the accuracy, confidentiality or integrity of the information is compromised and therefore is in violation of FIPPA or PHIA. Breaches may include, but are not limited to, the viewing of Confidential Information by unauthorized individuals, the access, theft or loss of WSD Records and the unauthorized destruction of such information by deliberate means or by human or natural accident.

15.2 All breaches are required to be reported immediately to the Access and Privacy Coordinator.

15.3 Any person associated with the WSD who becomes aware of a possible or actual Breach of Privacy, shall immediately report the possible or actual Breach of Privacy to the Access and Privacy Officer and/or Coordinator, who shall take immediate steps to contain the Breach.

15.4 All Breaches of Privacy will be investigated by the Access and Privacy Officer and Coordinator.

15.5 The Access and Privacy Officer and Coordinator will make recommendations for immediate and long-term corrective measures as necessary to protect the confidentiality, integrity and security of all Personal Information and Personal Health Information.

15.6 If it is determined that a Breach of Privacy has occurred, appropriate remedial action shall be taken by the WSD. Such action may include disciplinary action, which will be implemented pursuant to and in accordance with the relevant collective agreement, WSD policies or by-laws. The WSD may also consider notification of affected individuals and the Ombudsman's office, where notification is determined to be appropriate.

15.7 The Access and Privacy Officer and Coordinator will act as a resource for all persons associated with the WSD regarding appropriate action to be taken following a Breach of Privacy.

16. APPEAL PROCESS

16.1 If a parent/guardian, or a student over the age of 18, wishes to appeal the relevance or accuracy of any information contained in the pupil file, the following appeal process shall be followed:

(a) A written request, outlining the specifics of the appeal, shall be submitted to the Access and Privacy Coordinator;

(b) The Access and Privacy Officer and Coordinator shall review the information and render a decision, in writing, within two weeks of receipt of the requested appeal;

(c) The Access and Privacy Officer and Coordinator's decision may be appealed to the Board of Trustees by written request.