Message Start Event

Policy and Procedure Review

Policy and/or Procedure Name: * 5017 – Information Technology Policy / 5017a - Information Technology Security Procedure

New or Existing Policy/Procedure: *
- ○ New
- ◉ Existing

Who is expected to follow the procedure/to whom does the procedure apply/who is impacted? *
- ☑ Employees
- ☑ Students/Families/Parents/Guardians
- ☑ Trustees
- ☑ External groups/individuals to TVDSB

CONSULTATION

In considering those impacted, the following have been consulted in the development/revision of this policy/procedure:

Advisory Committees:
- ☐ Thames Valley Student Advisory Council (TVSAC)
- ☐ Thames Valley Parent Involvement Committee (TVPIC)
- ☐ Special Education Advisory Committee (SEAC)
- ☐ First Nations Advisory Committee (FNAC)

School Administrators:
- ☐ Thames Valley Secondary School Administrators' Council
- ☐ Thames Valley Administrators'Committee Elementary

Employee Groups
- ☑ CUPE 4222
- ☑ ETFO
- ☑ OSSTF
- ☑ AAPSP
- ☐ President's Council
- ☑ CUPE 7575
- ☑ OPC
- ☑ PSSP
- ☑ Manager's Association
- ☑ Other

CEI

Departments:

- [x] Human Resources
- [x] Finance
- [x] Learning Support Services
- [x] Facility Services
- [x] Corporate Services/Records
- [x] Communications
- [x] Diversity and Equity
- [x] Health and Safety
- [x] International Education
- [ ] Other

Other:

- [ ] Thames Valley Council of Home and School Associations
- [ ] Relevant Community Organizations
- [ ] Accessibility Working Group
- [ ] Indigenous Education Working Group
- [ ] Culture For Learning Advisory Committee (CFLAG)
- [ ] Other

In addition or instead of face to face consultation, I invited feedback by email from the following:

The Employee Groups and Departments, checked above, were emailed requesting feedback.

I recommend the following period of time for public input to gather additional feedback from the general community: *

- (•) None
- ( ) 30 days
- ( ) 60 days

Rationale:

Please note that 9037 – Corporate Email Procedure and 9056 – Use of Commercial Electronic Message Procedure have been consolidated into 5017 - Information Technology Policy and 5017a - Information Technology Security Procedure. Consequently, the rescission of Policies 9037 and 9056 is being requested.

EQUITY AND INCLUSION

The 2018-2021 TVDSB Strategic Plan states the Board's intention to: • Create opportunities for equitable access to programs and services for students • Ensure students and all partners feel heard, valued and supported • Provide programs and services that embrace the culture and diversity of students and all partners. With these strategic goals in mind, please consider the following with respect your policy/procedure.

The policy/procedure: *

- [ ] Draws a distinction between groups of individuals
- [ ] Treats certain individuals or groups differently than others
- [ ] Disproportionately disadvantages or negatively impacts any group or individual
- [ ] Confers a particular privilege or benefit on a group(s) not shared by others
- [x] None of the above

The policy/procedure relates to the delivery of a TVDSB program or service: *

- ( ) Yes
- (•) No

I anticipate challenges with respect to the implementation of this policy/procedure *

- ( ) Yes
- (•) No
- ( ) Unsure

RECORDS MANAGEMENT

There are forms, referred to in the procedure, that will be used to collect personal information *

- ( ) Yes
- (•) No

LEGAL

Legal consultation typically is not required for most policies and procedures. It you determine a legal review is required, for all or any part of the policy/procedure, please formulate the legal question you have in advance of approaching counsel.

Did you consult legal? *

- (•) No, it was not necessary
- ( ) Yes

SUBMITTING TO EIE

Submitted By: * Carolyn Glaser

Email: * C.GLASER@tvdsb.ca

Upload Documents: *	Please upload your policy and procedure documents here (word or pdf versions are accepted)	
	5017 Policy and 5017a Procedure.zip	2.22MB

Thames Valley District School Board
Equity & Inclusive Education
Review Summary

Name of Policy/Procedure:	Security Cameras and Digital Imagery Policy & Procedure
Policy/Procedure Number:	2017/a
Department Lead:	Carolyn Glaser, Jim Bobier
Originating Department:	Information Technology Services
Date of Submission to EIE:	March 14, 2024

EIE Review Committee comments and suggestions:
It is expected that the Administrative Procedure Holder (or designate) also document the Committee's comments and suggested changes during the Committee meeting

In regard to s. 2.3 of the Policy and Procedure, The Committee questioned who would constitute "authorized personnel" and whether that should be formalized and identified within the documents to ensure accountability and support the protection of privacy and personal information. The Policy Holder advised that it would be dependent on the location and specifics of the matter.

In regard to s. 5.1.2 of the Policy, the Committee recommended changing the American term "restroom" to the Canadian term "washroom".

In regard to s. 5.3.3.3 of the Procedure, the Committee emphasized the need for this amendment to come into force as soon as possible as the current procedure requires additional approval steps which may impede local authorities responding to an emergency (ie. a missing child).

In regard to s. 5.3.3.4 of the Procedure, the Committee noted the large amount of text and requested that larger sub-sections be shortened. It was suggested that this could be done by further dividing up s. 5 so that more of the page could be used.

In regard to s. 5.3.6.1 of the Procedure, the Committee questioned what the assessment entailed and whether this assessment criteria would be available / attached to the Procedure. The Policy Holder advised that there is not a specific assessment and that the determining factors would be determined at the time of the decision. The Committee raised concerns about the ability for bias to influence the process, the perception of bias, the lack of transparency, and the need for procedural fairness. The Policy Holder advised that she would be open to looking further into addressing these concerns.

In regard to s. 5.3.6.2 of the Procedure, the Committee noted that the current wording suggests that the Director of Education will approval all requests for covert surveillance and recommended changing the wording to say that "All requests for the use of covert surveillance will require approval by the Director of Education (or their designate)".

Thames Valley
District School Board

Security Cameras and Digital Imagery Policy

Policy Number:	2017
Policy Owner:	Information Technology Services
Effective Date:	2005 September 27
Amendment Dates:	2013 February 05, 2016 September 26
EIE Review Date:	2025 March 19
Resources:	• TVDSB Privacy and the Management of Personal Information Procedure (2014b) • TVDSB Privacy Breach Protocol Procedure (2014c) • TVDSB Security Cameras and Digital Imagery Procedure (2017a) • Municipal Freedom of Information and Privacy Act Ontario Regulation 823

1. Intent

1.1. Thames Valley District School Board (TVDSB) is committed to providing a safe and secure environment for students, staff, and visitors.

1.2. This policy outlines the use of security camera systems to monitor and record activities on school and site premises, aiming to deter and respond to incidents of misconduct, vandalism, and other security concerns while respecting individuals' privacy rights as defined by relevant privacy laws and regulations.

2. Definitions

2.1. **Security Camera System** is a video, physical or other mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing or monitoring of activities in TVDSB schools, and sites.

2.2. **Personal Information** is recorded information that can identify an individual. This includes details such as name, address, phone number, race, ethnic origin, religious or political beliefs or associations, age, sex, sexual orientation, mental status, family status, any identifying number or symbol (e.g., Social Insurance Number (SIN)), fingerprints, blood type, or inheritable characteristics. It also encompasses medical history, educational, financial, criminal, or employment history, personal views or opinions (unless they are about someone else), and anyone else's opinion about that individual.

2.3. **Authorized Personnel** are individuals designated by TVDSB to access security camera systems and recordings.

2.4. **Storage Device** stores visual, audio, or other data captured by a video surveillance system, and may include both on-premises and cloud-based infrastructure.

3. Objective of Policy

3.1. The objectives of this policy are to:

3.1.1. Enhance the safety and security of students, staff, and visitors.

3.1.2. Protect school property from theft, vandalism, and other forms of damage.

3.1.3. Support the investigation of incidents and enforcement of school policies.

3.1.4. Ensure compliance with applicable privacy laws and regulations, including the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

4. Roles and Responsibility

4.1. **Director of Education** is accountable for the security camera and digital imagery policy and procedure.

4.2. **General Manager of Information Technology Services** ensures that the installation, maintenance, and operation of security camera systems and digital imagery comply with this policy.

4.3. **Site Administrator or their designate** accesses and reviews video recordings as necessary for security and investigative purposes at their respective schools or sites and ensures staff and students are aware of the policy.

4.4. **Information Technology Services** provides technical support for the installation and maintenance of security camera systems.

4.5. **Records and Privacy Officer** ensures that the collection, use, and disclosure of personal information captured by security cameras comply with privacy laws and regulations.

4.6. **Freedom of Information Coordinator** ensures that requests for access by third parties and by individuals follows the board's process for releasing video recordings that may contain personal information.

4.7. **Authorized Personnel** access and review video recordings as necessary for security and investigative purposes.

5. Security Cameras and Digital Imagery Policy Directives

5.1. Installation and Placement:

5.1.1. Security camera systems should be used when a less intrusive means of deterrence has been implemented and proven to be ineffective.

5.1.2. Security camera systems will be installed in public areas such as hallways, entrances, and parking lots. Cameras will not be placed in areas where individuals have a reasonable expectation of privacy, for example, washrooms, classrooms, office spaces, prayer rooms and locker rooms.

5.1.3. The placement of cameras will be determined based on specific security needs and will be reviewed periodically to ensure effectiveness.

5.2. Notification:

5.2.1. Signs indicating the presence of security camera will be prominently displayed at school entrances and other monitored areas.

5.2.2. The signs will include contact information for inquiries about the security camera system.

5.3. Access and Use:

5.3.1. Access to security camera recordings will be restricted to authorized personnel. Recordings will be used solely for the purposes outlined in this policy.

5.3.2. Video recordings will not be used for monitoring staff performance or student behavior unless related to a specific incident under investigation.

5.3.3. Video recordings may be made available to the public through a Freedom of Information request. Information released will comply with the Municipal Freedom of Information and Protection of Privacy Act.

5.4. Retention and Disposal:

5.4.1. Video recordings will be retained for a period of 30 days, after which they will be securely deleted unless required for an ongoing investigation or legal proceedings.

5.4.2. Procedures for the secure disposal of recordings will be established to prevent unauthorized access.

5.5. Privacy and Confidentiality:

5.5.1. The collection, use, and disclosure of personal information captured by security camera will comply with applicable privacy laws and regulations.

5.5.2. Unauthorized access or disclosure of video recordings is strictly prohibited. Any breaches of privacy will be reported and addressed in accordance with TVDSB Privacy Breach Protocol Procedure (2014c).

5.6. Education and Awareness:

5.6.1. Education and awareness regarding staff obligations associated with the use and storage of electronic imagery and/or video footage shall be conducted as necessary.

6. Monitoring and Review

6.1. The monitoring and review of this Policy is based on the objectives outlined in Section 3.0. The ITS Department will be responsible for monitoring and reviewing this Policy to ensure alignment with legislative changes, information technology practices and/or Ministry of Education directives. The Information Technology Services Department will report on safeguarding personal and sensitive information and the promotion of safe online practices.

~~POLICY~~

~~Title VIDEO SURVEILLANCE~~ Security Cameras and Digital Imagery Policy ~~No.~~ ~~2017~~ ~~2005 Sept. 27~~

Policy Number:	2017
Policy Owner:	Information Technology Services
Effective Date:	2005 September 27
Amendment Dates:	2013 February 05, 2016 September 26
EIE Review Date:	2025 March 19
Resources:	• TVDSB Privacy and the Management of Personal Information Procedure (2014b) • TVDSB Privacy Breach Protocol Procedure (2014c) • TVDSB Security Cameras and Digital Imagery Procedure (2017a) • Municipal Freedom of Information and Privacy Act Ontario Regulation 823

~~Effective Date:~~

~~Department~~ ~~**Director's Services**~~

~~Reference(s)~~ ~~Procedure - Video Surveillance~~
~~Policy - Freedom of Information and Protection of Privacy~~
~~*Education Act*~~
~~*Municipal Freedom of Information and Privacy Act*~~
~~Ontario Regulation 823~~
~~Guidelines for the Use of Video Surveillance, IPC (2015)~~

~~1.0 Surveillance~~

~~It is the policy of the Board that video surveillance equipment shall be used in public areas of its schools and facilities or other areas as deemed necessary, and on third party service provider facilities (for example, school buses) only when it is deemed necessary to:~~

1. Intent

1.1. Thames Valley District School Board (TVDSB) is committed to providing a safe and secure environment for students, staff, and visitors.

1.2. This policy outlines the use of security camera systems to monitor and record activities on school and site premises, aiming to deter and respond to incidents of misconduct, vandalism, and other security concerns while respecting individuals' privacy rights as defined by relevant privacy laws and regulations.

2. Definitions

2.1. **Security Camera System** is a video, physical or other mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing or monitoring of activities in TVDSB schools, and sites.

2.2. **Personal Information** is recorded information that can identify an individual. This includes details such as name, address, phone number, race, ethnic origin, religious or political beliefs or associations, age, sex, sexual orientation, mental status, family status, any identifying number or symbol (e.g., Social Insurance Number (SIN)), fingerprints, blood type, or inheritable characteristics. It also encompasses medical history, educational, financial, criminal, or employment history, personal views or opinions (unless they are about someone else), and anyone else's opinion about that individual.

2.3. **Authorized Personnel** are individuals designated by TVDSB to access security camera systems and recordings.

2.4. **Storage Device** stores visual, audio, or other data captured by a video surveillance system, and may include both on-premises and cloud-based infrastructure.

3. Objective of Policy

3.1. The objectives of this policy are to:

~~1.1.1.~~3.1.1. Enhance the safety and ~~well-being~~security of students, staff, and ~~the~~

~~community;~~visitors.

- ~~1.1.2.~~Protect ~~Board~~school property ~~and equipment against~~from theft ~~or~~, vandalism~~;~~ 3.1.2. ~~aid in identifying intruders~~, and other forms of ~~persons breaking the law~~damage.

3.1.3. ~~The Board recognizes that any recorded data or visual, audio or other images of an identifiable individual falls within the definition~~Support the investigation of ~~"personal information" under~~ incidents and enforcement of school policies.

3.1.4. Ensure compliance with applicable privacy laws and regulations, including the Municipal Freedom of Information and Protection of Privacy Act ~~("~~(MFIPPA).

4. Roles and Responsibility

4.1. **Director of Education** is accountable for the ~~Act")~~security camera and digital imagery policy and procedure.

4.2. **General Manager of Information Technology Services** ensures that the installation, maintenance, and operation of security camera systems and digital imagery comply with ~~respect to notice, access~~this policy.

4.3. **Site Administrator or their designate** accesses and reviews video recordings as necessary for security and investigative purposes at their respective schools or sites and ensures staff and students are aware of the policy.

4.4. **Information Technology Services** provides technical support for the installation and maintenance of security camera systems.

4.5. **Records and Privacy Officer** ensures that the collection, use, and disclosure~~,~~ ~~retention,~~ of personal information captured by security cameras comply with privacy laws and regulations.

4.6. **Freedom of Information Coordinator** ensures that requests for access by third parties and by individuals follows the board's process for releasing video recordings that may contain personal information.

4.7. **Authorized Personnel** access and review video recordings as necessary for security and investigative purposes.

5. Security Cameras and Digital Imagery Policy Directives

5.1. Installation and Placement:

5.1.1. Security camera systems should be used when a less intrusive means of

deterrence has been implemented and proven to be ineffective.

5.1.2. Security camera systems will be installed in public areas such as hallways, entrances, and parking lots. Cameras will not be placed in areas where individuals have a reasonable expectation of privacy, for example, washrooms, classrooms, office spaces, prayer rooms and locker rooms.

5.1.3. The placement of cameras will be determined based on specific security needs and will be reviewed periodically to ensure effectiveness.

5.2. Notification:

5.2.1. Signs indicating the presence of security camera will be prominently displayed at school entrances and other monitored areas.

5.2.2. The signs will include contact information for inquiries about the security camera system.

5.3. Access and Use:

5.3.1. Access to security camera recordings will be restricted to authorized personnel. Recordings will be used solely for the purposes outlined in this policy.

5.3.2. Video recordings will not be used for monitoring staff performance or student behavior unless related to a specific incident under investigation.

5.3.3. Video recordings may be made available to the public through a Freedom of Information request. Information released will comply with the Municipal Freedom of Information and Protection of Privacy Act.

5.4. Retention and Disposal:

5.4.1. Video recordings will be retained for a period of 30 days, after which they will be securely deleted unless required for an ongoing investigation or legal proceedings.

~~1.1.3.~~5.4.2. Procedures for the secure disposal of ~~records containing personal information~~recordings will be established to prevent unauthorized access.

~~The collection of personal information shall be used only for the purposes of maintaining a safe environment, protecting school property or as required or permitted by law. The retention period for information that has not been viewed for law enforcement, school or public safety purposes shall be 30 calendar days following which it is to be routinely erased such that it cannot be reconstructed or retrieved.~~

~~The Director of Education/designate shall be responsible for the effective use of the surveillance system and the Board's privacy obligations for advising staff of the need to comply with the *Act* and policies.~~

~~Where video surveillance equipment is used, it shall be operated by the school principal or their designate and by the Director of Education or their designate in other Board facilities.~~

Thames Valley
District School Board

~~Video Surveillance Policy~~

~~Board employees shall have access to the personal information collected under the program only where necessary in the performance of their duties. They shall review and comply with the policy and the *Act* in performing any duties and functions related to the operation of the video surveillance program and in the collection and use of personal information. Employees shall be subject to discipline for knowingly or deliberately breaching the policy or the provisions of the *Act* or other relevant statutes.~~

~~The Board shall maintain control of, and responsibility for, the video surveillance system at all times.~~

~~2. 2.0 Third Party Service Providers~~

~~It is recognized that video surveillance equipment installed on third party facilities is the property of the third party if not provided or installed by the Board. The recorded information is the property of the Thames Valley District School Board. As operators of the equipment, service providers are responsible to comply with this policy in the collection, use, disclosure and security of personal information.~~

~~Agreements with third party providers shall state that any records dealt with or created pursuant to the video surveillance program are under the Board's control and are subject to the *Act*, and shall describe obligations for collection, use, disclosure, and security.~~

~~This policy shall be reviewed and updated every three years or earlier as appropriate.~~

5.5. ~~Page 2 of 2~~Privacy and Confidentiality:

5.5.1. The collection, use, and disclosure of personal information captured by security camera will comply with applicable privacy laws and regulations.

5.5.2. Unauthorized access or disclosure of video recordings is strictly prohibited. Any breaches of privacy will be reported and addressed in accordance with TVDSB Privacy Breach Protocol Procedure (2014c).

5.6. Education and Awareness:

5.6.1. Education and awareness regarding staff obligations associated with the use and storage of electronic imagery and/or video footage shall be conducted as necessary.

6. Monitoring and Review

6.1. The monitoring and review of this Policy is based on the objectives outlined in Section 3.0. The ITS Department will be responsible for monitoring and reviewing this Policy to ensure alignment with legislative changes, information technology practices and/or Ministry of Education directives. The Information Technology Services Department will report on safeguarding personal and sensitive information and the promotion of safe online practices.

Thames Valley
District School Board

Security Cameras and Digital Imagery

Procedure Number:	2017a
Procedure Owner:	Information Technology Services
Effective Date:	2005 September 27
Amendment Dates:	2013 February 5, 2016 September 26
EIE Review Date:	
Resources:	• TVDSB Privacy and Records Information Management (2014) • TVDSB Records Information Management Procedure (2014a) • TVDSB Privacy and the Management of Personal Information Procedure (2014b) • TVDSB Privacy Breach Protocol Procedure (2014c) • TVDSB Security Cameras and Digital Imagery Policy (2017) • TVDSB Information Technology Appropriate Usage and Electronic Monitoring Procedure (5017b) • Municipal Freedom of Information and Privacy Act Ontario Regulation 823

1. Intent

1.1. The intent of this procedure is to ensure the safety and security of students, staff, and visitors at Thames Valley District School Board (TVDSB) sites and schools. This procedure aims to deter and prevent acts of vandalism, theft, and other criminal activities by providing a visible and effective monitoring system.

1.2. Additionally, the procedure is designed to comply with relevant privacy laws and regulations, ensuring that the collection, retention, use, and disclosure of personal information are conducted lawfully and ethically.

2. Definitions

2.1. **Auditable Log** is a detailed record that tracks user activities and system operations. It typically includes information such as the identity of the user, the actions performed, the time and date of those actions, and any changes made to the system.

2.2. **Authorized Agency** refers to any duly constituted criminal investigative department or agency, such as law enforcement, regulatory bodies, or other governmental entities, that has the legal authority to access and use certain information or perform specific actions.

2.3. **Authorized Personnel** are individuals designated by TVDSB to access security camera systems and recordings.

2.4. **Covert Surveillance** is surveillance conducted by means of hidden devices, without notice to the individual(s) being monitored on TVDSB property or within TVDSB buildings.

2.5. **Electronic Imagery** refers to the creation, processing, storage, and display of digital representations of visual characteristics of objects. This includes digital photographs, videos, and other forms of digital images stored and/or administered TVDSB infrastructure, equipment and/or devices that can be manipulated and analyzed using computer software.

2.6. **Personal Information** is recorded information that can identify an individual. This includes details such as name, address, phone number, race, ethnic origin, religious or political beliefs or associations, age, sex, sexual orientation, mental status, family status, any identifying number or symbol (e.g., Social Insurance Number (SIN)), fingerprints, blood type, or inheritable characteristics. It also encompasses medical history, educational, financial, criminal, or employment history, personal views or opinions (unless they are about someone else), and anyone else's opinion about that individual.

2.7. **Record** is any information, however recorded, whether in printed form, on film, by electronic means, or otherwise. This includes a photograph, a film, a microfilm, and a videotape.

2.8. **Storage Device** stores visual, audio, or other data captured by a security camera system, and may include both on-premises and cloud-based infrastructure.

2.9. **Security Camera System** is a video, physical or other mechanical, electronic, digital system or device that is administered by Information Technology Services staff and enables continuous or periodic video recording, observing or monitoring of activities in TVDSB schools and sites.

2.10. **Video footage** refers to the recorded data captured by a security system or security camera. This includes visual, audio, or other images electronically stored.

3. Objective of Procedure

3.1. The objectives of the TVDSB video security camera procedure:

3.1.1. To maintain transparency in the use of security video systems and ensure accountability in their operation and management.

3.1.2. To ensure that the security video system operates in accordance with relevant privacy laws and regulations, collecting only the data necessary to achieve the intended goals.

3.1.3. To manage the collection, retention, use, and disclosure of video footage data in a lawful and ethical manner, ensuring the protection of personal information.

4. Roles and Responsibility

4.1. **General Manager of Information Technology Services** ensures that the installation, maintenance, and operation of security camera systems and digital imagery comply with this procedure.

4.2. **Information Technology Services** provides technical support for the installation and maintenance of security camera systems.

4.3. **Site Administrators or Designates** are responsible for operating the security camera system at their respective TVDSB schools or non-school sites.

4.4. **Records and Privacy Officer** ensures that the collection, use, and disclosure of personal information captured by security cameras comply with privacy laws and regulations.

4.5. **Security Camera Committee** is a committee consisting of TVDSB staff from various board departments such as Human Resource, Information Technology Services, Facilities, Safe Schools and School Administration, which review and prioritize the allocation of security cameras for new deployments and replacements of existing systems at board locations across the district, in alignment and adherence with the Thames Valley District School Board Security Cameras and Digital Imagery Policy (2017) and this procedure.

4.6. **Freedom of Information Coordinator** ensures that requests for access by third parties and by individuals follows the board's process for releasing video recordings that may contain personal information.

5. Security Cameras and Digital Imagery Procedures

5.1. Included below Sections 6 through 13 are the TVDSB are the Security Cameras and Digital Imagery Procedures

6. Considerations Prior to Using Security Cameras:

6.1. Before implementing security cameras at a school or other location the Principal or Site Administrator or designates working with the Security Camera Committee will:

6.1.1. consider use of security cameras when less intrusive means of deterrence has been implemented and proven to be ineffective.

6.1.2. provide evidence of incidents occurring in the school or site to justify the use and extent of use of security camera equipment to deal with or prevent future incidents. Where security cameras are being deployed for secured controlled access to TVDSB buildings and sites, provision of evidence of incidents will not be required.

7. Design, Installation and Operating Security Cameras:

7.1. Design and positioning of the approved security cameras will be determined in consultation with the Principal or Site Administrator or designates, the General Manager of Information Technology Services or designate and other TVDSB staff as deemed appropriate.

7.2. In designing, installing and operating security cameras, TVDSB will:

7.2.1. install equipment only in identified public areas where security cameras are considered necessary to ensure the safety of students, staff, and TVDSB property.

7.2.2. ensure that the proposed design and operation of the security cameras minimize privacy intrusion to that which is necessary to provide protection and safety.

7.2.3. equipment will not be set up in areas where students, staff, and the public have an expectation of privacy (e.g., washrooms, classrooms, office spaces, prayer rooms and locker rooms).

7.2.4. prominently display signs at the entrances and/or the interior and/or exterior of buildings and on third party service provider where TVDSB security cameras are operating to provide students, staff, and the public with reasonable and adequate notice and inform them that they may contact the Site Administrator or TVDSB's Privacy Officer with any questions about the collection of security camera footage (Appendix A).

7.2.5. ensure all security cameras are maintained and operating as expected.

7.2.6. the Principal or Site Administrator or their designates will be responsible for reporting to the Information Technology Services Department through their service support management system any issues or concerns regarding the performance of such equipment.

7.2.7. operate the security equipment 24 hours each day, 7 days a week, within the limitations of system capabilities, power disruptions and maintenance

periods.

8. Electronic Imagery and Video Footage

8.1. Included below in Sections 9 through 14 are the procedures for the use, security, access, disclosure, retention and disposal of electronic imagery and video footage.

9. Use of Electronic Imagery and Video Footage

9.1. Any electronic imagery and video footage information obtained by way of a security camera and/or other device administered by Information Technology Services may be used in accordance with this with TVDSB Security Cameras and Digital Imagery Policy (2017) and this procedure.

9.2. Third party service providers that have electronic imagery and/or video footage services and/or equipment installed, must sign an agreement satisfactory to TVDSB regarding the collection, use, disclosure and security of the personal information collected that complies with this policy and procedure.

9.3. A Privacy Impact Assessment (PIA) will be completed before the TVDSB enters into an agreement with any third-party service provider.

9.4. Viewing of electronic imagery and/or video footage shall be in accordance with this procedure. Circumstances which warrant review will be limited to an incident that has been reported or observed, to investigate a potential crime, or in response to Freedom of Information request.

9.5. Electronic imagery and/or video footage may be accessed to investigate matters related to staff and student conduct that are likely to result in a law enforcement and/or TVDSB investigation.

9.6. This procedure is not meant to address or apply to instances where staff electronically record and/or capture a specific event (such as a school performance, graduation ceremony or field trips).

10. Security of Records

10.1. Storage devices and repositories containing electronic imagery and/or video footage are to be stored securely with access limited by the Principal or Site Administrator or their designates and other Authorized Personnel.

11. Accessing Electronic Imagery and Video Footage

11.1. Site Administrator or designates and Authorized Personnel will ensure that electronic imagery and/or video footage is accessible only to Authorized Personnel.

11.2. If electronic imagery or video footage is needed to resolve a security or safety issue, or to respond to a Freedom of Information request, it will be securely stored for a length of time according to the retention schedule outlined in the TVDSB Records Information Management Procedure (2014a).

11.3. Site Administrator or designates and Authorized Personnel shall ensure that any recorded electronic imagery and/or video footage accessed or disclosed by Authorized Personnel is dated with a unique, sequential number or other verifiable symbol (e.g., watermark).

11.3.1. A log will be maintained to record all instances of access to, and use of, recorded material.

11.3.2. This does not apply to the viewing of a live feed of electronic imagery and/or video footage.

11.4. When real-time viewing of the electronic imagery and/or video footage is necessary, the authority to view the data will be granted by the Principal or Site Administrator or their designates to authorized personnel to assist in resolving a security and/or safety issue.

11.5. Electronic imagery and/or video footage will not be viewable by the public.

11.6. Individuals whose personal information has been collected by a TVDSB electronic imagery and/or video footage device have the right of access to their personal information under Section 36 of Municipal Freedom of Information and Privacy Act Ontario Regulation 823.

11.7. Access may be granted to an individual's own personal information in whole or in part, unless an exemption applies under Section 38 to Municipal Freedom of Information and Privacy Act Ontario Regulation 823 where, for example, disclosure would constitute an unjustified invasion of another individual's privacy.

11.8. Access to an individual's own personal information may also depend upon whether any exempt information can be reasonably severed from the record. Requests for access to electronic imagery and/or video footage must be requested through the TVDSB's Freedom of Information request process.

11.9. **Authorizing the Release of Imagery and Video Footage**

11.9.1. Viewing of recorded information will be limited to the Site Administrator or their designates, Authorized Personnel, and Authorized Agencies as required or permitted by law, where necessary.

11.9.2. Circumstances that warrant viewing will be limited to an incident that has been reported/observed, to investigate a potential crime, or in response to a Freedom of Information request.

11.9.3. Electronic imagery and/or video footage may be disclosed to an Authorized Agency under the following circumstances. In all cases, an auditable log will be completed by the Principal or Site Administrator or their designates and shared with the TVDSB's Records and Privacy Officer.

11.9.3.1. The Authorized Agency approaches the Principal or Site Administrator or their designates or Information Technology Services General Manager with a warrant and/or production order requiring the disclosure of the electronic imagery and/or video footage.

11.9.3.2. The Authorized Agency approaches the Site Administrator or their designates or Information Technology Services General Manager, without a warrant or production order, and requests the electronic imagery and/or video footage be disclosed to aid an investigation from which a proceeding is likely to result.

11.9.3.3. An activity that endangers health and safety of staff and/or students has occurred on TVDSB property and the electronic imagery and/or

video footage is disclosed to an Authorized Agency to aid an investigation.

11.9.4. The Site Administrator or their designate will ensure record of the electronic transmission of video electronic imagery and/or video footage is maintained, when this information is disclosed to Authorized Personnel.

11.9.5. Any unauthorized viewing or disclosures of personal information shall be reported immediately to the TVDSB's Privacy Officer. The matter shall be investigated as per TVDSB Privacy Breach Protocol Procedure (2014c).

12. Covert Surveillance

12.1. Covert surveillance, such as hidden cameras or cameras installed without notification, is highly privacy-invasive and is not a standard practice of Thames Valley District School Board (TVDSB). It will only be used as a last resort in limited, case-specific circumstances.

12.2. All requests for covert surveillance must be submitted to the Director of Education or their designate for approval.

12.2.1. The request must clearly describe the rationale and the timelines for the surveillance.

12.2.2. A review of the request will be conducted to evaluate the privacy impacts associated with the implementation of covert surveillance.

12.2.3. This review aims to ensure that covert surveillance is the only available option under the circumstances and that the benefits derived from the personal information obtained outweigh the violation of privacy of the individual(s) observed.

13. Monitoring and Review

13.1. The monitoring and review of this Procedure is based on the objectives outlined in Section 3.0.

13.2. The Information Technology Services Department will be responsible for monitoring, reviewing and recommending changes to this Procedure to ensure alignment with

legislative changes, information technology practices and/or Ministry of Education directives.

14. List of Appendices

14.1. Appendix A: Notice of Security Camera Monitoring and Collection of Data

Appendix A – Notice of Security Camera Monitoring and Collection of Data

The following will be located at the entrances of all TVDSB buildings.

This property is monitored by 24-hour security camera technology.

Security cameras are in operation for the safety of the students, staff and the school community and for the protection of Thames Valley District School Board property. Information is collected under the authority of the Education Act in compliance with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). For additional information please contact the Principal/Supervisor of this site.

Contact information is available in the office/front desk or visit our website – www.tvdsb.ca.

~~1. PROCEDURE~~

~~Title~~	**~~VIDEO SURVEILLANCE~~**	~~Procedure No.~~	**~~2017a~~**
		~~Effective Date:~~	**~~2005 Sept. 27~~**

~~Department~~ **~~Director's Services~~**

~~Reference(s)~~ ~~Policy - Video Surveillance~~
~~Policy - Freedom of Information and Protection of Privacy~~
~~*Education Act*~~
~~*Municipal Freedom of Information and Privacy Act*~~
~~Ontario Regulation 823~~
~~Guidelines for the Use of Video Surveillance, IPC (2015)~~

~~The following procedures provide Board and school administrators with the steps to implement and maintain a video surveillance system in accordance with legislation and the guidelines provided by the Information and Privacy Commission/Ontario. They are not intended to deal with instances where special events, such as graduation ceremonies, are videotaped or where a classroom is videotaped for educational or research purposes.~~

~~The Director of Education or designate will be responsible for advising school staff of the need to comply with the provisions of this policy and procedure in accordance with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). School administrators will be responsible for use of the equipment and for the privacy obligations under MFIPPA.~~

~~Any agreements between the Board and service providers will indicate that the records dealt with or created while using a video surveillance program will remain under the Board's control and subject to MFIPPA.~~

Administered By:	**DIRECTOR'S SERVICES**
Amendment Date(s):	2013 Feb. 5, 2016 Sept. 26

~~A. OVERT SURVEILLANCE~~

~~1.0 Use of~~Security Cameras and ~~Monitors (Non-Recording Devices)~~Digital Imagery

Procedure Number:	2017a
Procedure Owner:	Information Technology Services
Effective Date:	2005 September 27
Amendment Dates:	2013 February 5, 2016 September 26
EIE Review Date:	
Resources:	• TVDSB Privacy and Records Information Management (2014) • TVDSB Records Information Management Procedure (2014a) • TVDSB Privacy and the Management of Personal Information Procedure (2014b) • TVDSB Privacy Breach Protocol Procedure (2014c) • TVDSB Security Cameras and Digital Imagery Policy (2017) • TVDSB Information Technology Appropriate Usage and Electronic Monitoring Procedure (5017b) • Municipal Freedom of Information and Privacy Act Ontario Regulation 823

~~Cameras and monitors (non-recording devices) may be installed in schools and facilities for the purposes of ensuring the ongoing~~

1. Intent

The intent of this procedure is to ensure the safety and security of students, staff, and ~~property.~~

1.1. ~~In designing, installing and operating a~~ visitors at Thames Valley District School Board (TVDSB) sites and schools. This procedure aims to deter and prevent acts of vandalism, theft, and other criminal activities by providing a visible and effective monitoring system ~~for security, the Administration will follow procedures outlined in~~

~~Section 3.0.~~.

~~**2.0 Deciding to Use a Video Surveillance System (Recording Devices)**~~

1.2. Additionally, the procedure is designed to comply with relevant privacy laws and regulations, ensuring that the collection, retention, use, and disclosure of personal information are conducted lawfully and ethically.

2. Definitions

2.1. **Auditable Log** is a detailed record that tracks user activities and system operations. It typically includes information such as the identity of the user, the actions performed, the time and date of those actions, and any changes made to the system.

2.2. **Authorized Agency** refers to any duly constituted criminal investigative department or agency, such as law enforcement, regulatory bodies, or other governmental entities, that has the legal authority to access and use certain information or perform specific actions.

2.3. **Authorized Personnel** are individuals designated by TVDSB to access security camera systems and recordings.

2.4. **Covert Surveillance** is surveillance conducted by means of hidden devices, without notice to the individual(s) being monitored on TVDSB property or within TVDSB buildings.

2.5. **Electronic Imagery** refers to the creation, processing, storage, and display of digital representations of visual characteristics of objects. This includes digital photographs, videos, and other forms of digital images stored and/or administered TVDSB infrastructure, equipment and/or devices that can be manipulated and analyzed using computer software.

2.6. **Personal Information** is recorded information that can identify an individual. This includes details such as name, address, phone number, race, ethnic origin, religious or political beliefs or associations, age, sex, sexual orientation, mental status, family status, any identifying number or symbol (e.g., Social Insurance Number (SIN)), fingerprints, blood type, or inheritable characteristics. It also encompasses medical history, educational, financial, criminal, or employment history, personal views or opinions (unless they are about someone else), and anyone else's opinion about that individual.

2.7. **Record** is any information, however recorded, whether in printed form, on film, by electronic means, or otherwise. This includes a photograph, a film, a microfilm, and a videotape.

2.8. **Storage Device** stores visual, audio, or other data captured by a security camera system, and may include both on-premises and cloud-based infrastructure.

2.9. **Security Camera System** is a video, physical or other mechanical, electronic, digital system or device that is administered by Information Technology Services staff and enables continuous or periodic video recording, observing or monitoring of activities in TVDSB schools and sites.

2.10. **Video footage** refers to the recorded data captured by a security system or security camera. This includes visual, audio, or other images electronically stored.

3. Objective of Procedure

3.1. The objectives of the TVDSB video security camera procedure:

3.1.1. To maintain transparency in the use of security video systems and ensure accountability in their operation and management.

3.1.2. To ensure that the security video system operates in accordance with relevant privacy laws and regulations, collecting only the data necessary to achieve the intended goals.

3.1.3. To manage the collection, retention, use, and disclosure of video footage data in a lawful and ethical manner, ensuring the protection of personal information.

4. Roles and Responsibility

4.1. **General Manager of Information Technology Services** ensures that the installation, maintenance, and operation of security camera systems and digital imagery comply with this procedure.

4.2. **Information Technology Services** provides technical support for the installation and maintenance of security camera systems.

4.3. **Site Administrators or Designates** are responsible for operating the security camera system at their respective TVDSB schools or non-school sites.

4.4. **Records and Privacy Officer** ensures that the collection, use, and disclosure of personal information captured by security cameras comply with privacy laws and regulations.

4.5. **Security Camera Committee** is a committee consisting of TVDSB staff from various board departments such as Human Resource, Information Technology Services, Facilities, Safe Schools and School Administration, which review and prioritize the allocation of security cameras for new deployments and replacements of existing systems at board locations across the district, in alignment and adherence with the Thames Valley District School Board Security Cameras and Digital Imagery Policy (2017) and this procedure.

4.6. **Freedom of Information Coordinator** ensures that requests for access by third parties and by individuals follows the board's process for releasing video recordings that may contain personal information.

5. Security Cameras and Digital Imagery Procedures

5.1. Included below Sections 6 through 13 are the TVDSB are the Security Cameras and Digital Imagery Procedures

6. Considerations Prior to Using Security Cameras:

~~1.2.~~6.1. Before implementing ~~a video surveillance system, school and Board administration~~security cameras at a school or other location the Principal or Site Administrator or designates working with the Security Camera Committee will:

~~1.2.1.~~6.1.1. consider use of ~~a system only where~~ security cameras when less intrusive means of deterrence~~, such as increased monitoring by teachers, have~~ has been ~~shown~~implemented and proven to be ineffective~~ or unworkable;~~.

~~1.2.2.~~6.1.2. ~~be able to demonstrate a history~~provide evidence of incidents occurring in the school~~/Board facility~~ or site to justify the use and extent of use of ~~the~~security camera equipment to deal with or prevent future incidents~~;~~. Where security cameras are being deployed for secured controlled access to TVDSB buildings and sites, provision of evidence of incidents will not be required.

~~2.1 consider if the site permits ready access to unauthorized individuals and if there are specific safety issues involving the site;~~

~~2.2 consider the effects that the surveillance system will have on personal privacy and the ways in which such adverse effects may be mitigated;~~

2.3 provide information to the School Council, and Home and School Association as to the need for a video surveillance program outlining the less intrusive means that have been considered and the reason why they have not been effective; and

2.4 consider input from the School Council, Home and School Association, parents, staff, students and the broader community for a video surveillance program.

Information documenting the above shall be in writing and submitted to the school superintendent.

It is the responsibility of the school superintendent to approve the video surveillance system and to notify Facility Services as appropriate.

2.7. Design, Installation and Maintaining Video Surveillance EquipmentOperating Security Cameras:

2.1.7.1. All camera locations shall be authorized by Design and positioning of the schoolapproved security cameras will be determined in consultation with the Principal or Director of Education/Site Administrator or designates, the General Manager of Information Technology Services or designate in consultation with Facility services and and other stakeholdersTVDSB staff as deemed appropriate.

2.2.7.2. In designing, installing and operating a video security surveillance system, the Administrationcameras, TVDSB will:

2.2.1.7.2.1. install reception equipment only in identified public areas where surveillance issecurity cameras are considered necessary to ensure the safety of students, staff, and schoolTVDSB property. The equipment may operate continually if deemed necessary, or may be limited to the periods of concern;

2.2.2.7.2.2. ensure that the proposed design and operation of the surveillance system minimizessecurity cameras minimize privacy intrusion to that which is absolutely necessary to provide protection and safety.

2.2.3.7.2.3. equipment will not be set up in areas where students, staff, and the public have an expectation of privacy (e.g., changewashrooms, classrooms, office spaces, prayer rooms and washrooms);locker rooms).

3.0 provide notice informing the parents/guardians or adult students of the installation (see Appendix B); and

7.2.4. prominently display signs , as provided through Facilities, at the entrances

and/or the interior and/or exterior of buildings and on third party service provider ~~facilities (such as school buses) having video~~where TVDSB security ~~surveillance systems~~cameras are operating to provide students, staff, and the public with reasonable and adequate notice ~~that~~and inform them that they may contact the Site Administrator or TVDSB's Privacy Officer with any questions about the collection of security camera footage (Appendix A).

7.2.5. ensure all security cameras are maintained and operating as expected.

7.2.6. the Principal or Site Administrator or their designates will be responsible for reporting to the Information Technology Services Department through their service support management system any issues or concerns regarding the performance of such equipment.

7.2.7. operate the security equipment 24 hours each day, 7 days a week, within the limitations of system capabilities, power disruptions and maintenance periods.

8. Electronic Imagery and Video Footage

8.1. Included below in Sections 9 through 14 are the procedures for the use, security, access, disclosure, retention and disposal of electronic imagery and video footage.

9. Use of Electronic Imagery and Video Footage

~~3.1~~ Any electronic imagery and video ~~surveillance is in effect and informing them that they may contact the school office or the Board's Freedom of Information Co-ordinator with any questions about the collection.~~

~~4.0 Use, Security, Access, Disclosure, Retention and Disposal of Video Security Surveillance Records~~

~~4.1 Use of Surveillance~~

~~2.3.~~9.1. ~~Any~~footage information obtained by way of ~~video surveillance systems~~ a security camera and/or other device administered by Information Technology Services may be used in accordance with this ~~policy~~with TVDSB Security Cameras and Digital Imagery Policy (2017) and this procedure.

~~4.1.1 Each September notice will be provided to parents from the school advising them of the use of video surveillance equipment in the school and/or on a school bus serving the school.~~

~~4.1.2 Third Party Service Providers:~~

~~2.4.~~9.2. Third party service providers~~,~~ that have electronic imagery and/or video ~~surveillance~~footage services and/or equipment installed, must sign an agreement satisfactory to ~~the Board~~TVDSB regarding the collection, use, disclosure and security of the personal information collected that complies with this policy and procedure.

9.3. A Privacy Impact Assessment (PIA) will be completed before the TVDSB enters into an agreement with any third-party service provider.

~~2.5.~~9.4. Viewing of ~~the~~ electronic imagery and/or video ~~surveillance~~footage shall be in accordance with ~~section 4.3 of~~ this procedure. Circumstances which warrant review will be limited to an incident that has been reported or observed, ~~or~~ to investigate a potential crime~~. Third party service providers shall have a policy and procedure regarding the Use~~, or in response to Freedom of ~~Video Surveillance Equipment posted publically on their website~~Information request.

~~4.1.3 Video surveillance will not be used to monitor general staff performance.~~

2.6.9.5. Video surveillance Electronic imagery and/or video footage may be accessed to investigate matters related to staff and student conduct that are likely to result in a law enforcement and/or BoardTVDSB investigation.

9.6. This procedure is not meant to address or apply to instances where staff electronically record and/or capture a specific event (such as a school performance, graduation ceremony or field trips).

3.10. Security of Records

To protect the recorded personal information, school administrators will ensure that all Storage devices that are not in use are and repositories containing electronic imagery and/or video footage are to be stored securely in a locked and secure location with access to the storage devices limited to the school administrative staff.

4.2 Access

3.1.10.1. There shall be no access to video surveillance by third party service providers except as authorizedthe Principal or Site Administrator or their designates and other Authorized Personnel.

11. The principal of the schoolAccessing Electronic Imagery and Video Footage

11.1. Site Administrator or designates and Authorized Personnel will ensure that theelectronic imagery and/or video surveillance equipment and storage devices arefootage is accessible only to Authorized Personnel and that access to the equipment by others is prohibited. .

3.2.11.2. If itelectronic imagery or video footage is necessaryneeded to view tapes to assist in resolvingresolve a security or safety issue, they will be kept in a locked, secured areaor to respond to a Freedom of Information request, it will be securely stored for a one-year period from the datelength of resolution of the incident.time according to the retention schedule outlined in the TVDSB Records Information Management Procedure (2014a).

11.3. The principalSite Administrator or designates and Authorized Personnel shall ensure that any recorded electronic imagery and/or video footage accessed or disclosed by

Authorized Personnel is dated ~~and labeled~~ with a unique, sequential number or other verifiable symbol~~.~~ (e.g., watermark).

~~3.2.1.~~11.3.1. A log will be maintained to record all instances of access to, and use of, recorded material.

~~3.2.2.~~11.3.2. This does not apply to the viewing of a live feed~~.~~ of electronic imagery and/or video footage.

~~3.3.~~11.4. ~~Where~~When real-time viewing of the ~~monitors~~electronic imagery and/or video footage is necessary, the authority to view the ~~monitors may~~data will be ~~delegated only~~granted by the ~~Director of Education/designate~~Principal or ~~principal~~Site Administrator or their designates to authorized personnel to assist in resolving a security and/or safety issue.

11.5. Electronic imagery and/or video footage will not be viewable by the public.

11.6. Individuals whose personal information has been collected by a ~~video surveillance system~~TVDSB electronic imagery and/or video footage device have the right of access to their personal information under Section 36 of ~~*MFIPPA.*~~ Municipal Freedom of Information and Privacy Act Ontario Regulation 823.

~~3.4.~~11.7. Access may be granted to an individual's own personal information in whole or in part, unless an exemption applies under Section 38 to Municipal Freedom of ~~the~~Information and Privacy Act Ontario Regulation 823 where, for example, disclosure would constitute an unjustified invasion of another individual's privacy.

~~3.5.~~11.8. ~~constitute an unjustified invasion of another individual's privacy.~~ Access to an individual's own personal information may also depend upon whether any exempt information can be reasonably severed from the record. Requests for access to electronic imagery and/or video footage must be requested through the TVDSB's Freedom of Information request process.

~~4.3 Disclosure~~

11.9. Authorizing the Release of Imagery and Video Footage

~~3.5.1.~~11.9.1. Viewing of recorded information will be limited to the ~~school administrators/designate, the appropriate supervisory officer(s) and law enforcement officials~~Site Administrator or their designates, Authorized

Personnel, and Authorized Agencies as required or permitted by law, where necessary.

~~3.5.2.~~11.9.2. Circumstances that warrant viewing will be limited to an incident that has been reported/observed ~~or~~, to investigate a potential crime, or in response to a Freedom of Information request.

~~4.3.1 Video surveillance may be disclosed to a law enforcement agency when:~~

11.9.3. Electronic imagery and/or video footage may be disclosed to an Authorized Agency under the following circumstances. In all cases, an auditable log will be completed by the Principal or Site Administrator or their designates and shared with the TVDSB's Records and Privacy Officer.

~~3.5.2.1.~~11.9.3.1. The ~~law enforcement~~Authorized Agency approaches the ~~school~~Principal or Site Administrator or their designates or Information Technology Services General Manager with a warrant and/or production order requiring the disclosure of the electronic imagery and/or video footage~~;~~.

~~3.5.2.2.~~11.9.3.2. The ~~law enforcement~~Authorized Agency approaches the ~~school~~Site Administrator or their designates or Information Technology Services General Manager, without a warrant or production order, and requests the electronic imagery and/or video footage be disclosed to aid an investigation from which a proceeding is likely to result~~; or~~.

~~3.5.2.3.~~11.9.3.3. An ~~illegal~~ activity ~~is observed~~that endangers health and safety of staff and/or students has occurred on ~~school~~TVDSB property and the electronic imagery and/or video footage is disclosed to ~~a law enforcement~~an Authorized Agency to aid an investigation ~~from which a proceeding is likely to result.~~.

~~4.3.2 The principal will ensure a Storage Device Release form is completed before any storage device is disclosed to appropriate authorities. The form will indicate who took the device, under what authority, when this occurred, and if it will be returned or destroyed after use.~~

11.9.4. The Site Administrator or their designate will ensure record of the electronic transmission of video electronic imagery and/or video footage is maintained, when this information is disclosed to Authorized Personnel.

~~3.5.3.~~11.9.5. Any unauthorized viewing or disclosures of personal information shall be reported immediately to the ~~Freedom of Information Co-ordinator.~~TVDSB's Privacy Officer. The matter shall be investigated as per ~~*Handling a*~~TVDSB Privacy Breach ~~under the Privacy and Access~~Protocol Procedure~~.~~ (2014c).

~~4.4 Retention of Recorded Information~~

~~4.4.1 The retention period for information that has not been viewed for law enforcement, school or public safety purposes shall be 30 calendar days~~

following which it is to be routinely erased such that it cannot be reconstructed or retrieved. The retention periods are to be clearly documented at schools/facilities using video surveillance systems.

The retention period for storage devices used by third party service providers shall be four school days after which they shall be erased, except in circumstances where they are required by the Principal for investigative action.

4.4.2 When recorded information has been viewed the retention period shall be the longer of one year from the date of viewing or for one year from the date of resolution of the incident in accordance with Section 5 of Ontario Regulation 823 under *MFIPPA*.

4.5 Disposal

Storage devices having met their retention requirements must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved. Disposal methods could include shredding, burning or magnetically erasing the personal information. The principal will ensure a record of the date of disposal of each storage device is maintained in a log.

~~**5.0 Auditing and Evaluating the Use of a Video Surveillance System**~~

12. ~~The use and security of video surveillance equipment~~Covert Surveillance

12.1. Covert surveillance, such as hidden cameras or cameras installed without notification, is highly privacy-invasive and is not a standard practice of Thames Valley District School Board (TVDSB). It will only be used as a last resort in limited, case-specific circumstances.

12.2. All requests for covert surveillance must be submitted to the Director of Education or their designate for approval.

12.2.1. The request must clearly describe the rationale and the timelines for the surveillance.

~~5.1~~ A review of the request will be ~~subject to regular audits by Director's Services/designate to determine a) compliance with Board policy and procedures, and b) the necessity to continue a video surveillance program operating in schools or other facility. Any concerns identified by the audit will be addressed by Administration in a timely fashion.~~

~~6.0 **Training**~~

~~Where applicable and appropriate, the policy and procedure will be incorporated into training and orientation programs of the Board or service provider. Training programs addressing staff obligations and how real-time and recorded information viewing may be carried out under the *Act* shall be~~ conducted ~~on a regular basis.~~

~~**B. COVERT SURVEILLANCE**~~

~~**1.0 Needs Assessment**~~

12.2.2. ~~Prior to deciding to use covert surveillance, a comprehensive assessment of~~to evaluate the privacy impacts associated with the implementation of ~~such as program will be conducted. The assessment will~~covert surveillance.

~~3.5.4.~~12.2.3. This review aims to ensure that covert surveillance is ~~deemed appropriate in~~the only available option under the circumstances and that the benefits derived from the personal information obtained outweigh the violation of privacy of the ~~individuals~~individual(s) observed~~,~~.

~~e.g. an ongoing computer theft where other investigative techniques have been attempted and have failed.~~

~~1.1 The school principal will consult with the school Superintendent and may also~~

~~consult with law enforcement agencies, as appropriate to determine if covert surveillance measures are necessary and recommended. In all cases where covert surveillance takes place, it will be limited to a specific time frame and used as a case-specific investigation tool.~~

~~**1.1 2.0 Security of Records**~~

13. ~~**To protect the recorded personal information, school administrators will ensure that**~~ **Monitoring and Review**

13.1. The monitoring and review of this Procedure is based on the objectives outlined in Section 3.0.

13.2. The Information Technology Services Department will be responsible for monitoring, reviewing and recommending changes to this Procedure to ensure alignment with legislative changes, information technology practices and/or Ministry of Education directives.

14. List of Appendices

14.1. Appendix A: Notice of Security Camera Monitoring and Collection of Data

Appendix A – Notice of Security Camera Monitoring and Collection of Data

The following will be located at the entrances of all TVDSB buildings.

This property is monitored by 24-hour security camera technology.

Security cameras are in operation for the ~~storage device is stored in a locked and secure location with access to~~ safety of the ~~storage device limited to~~ students, staff and the school ~~administration.~~

~~3.0 Viewing~~community and ~~Disclosure~~

~~3.1 Viewing of recorded information through covert surveillance will be limited to~~for the ~~school administrators, the appropriate supervisory officer(s) and law enforcement officials where necessary, or as required or permitted by law.~~

~~3.2 Any unauthorized viewing or disclosures of personal information shall be reported immediately to the Freedom of Information Co-ordinator. The matter shall be investigated as per *Handling a Privacy Breach*~~ protection of Thames Valley District School Board property. Information is collected under the ~~Privacy and Access Procedure.~~

3.3 The dates and times of surveillance periods and police occurrence numbers will be logged and maintained by the school. Documentation shall be submitted to the school Superintendent.

3.4 Any storage device that has been used by authorized personnel will be dated and labeled with a unique, sequential number or other verifiable symbol. A log will be maintained to record all instances of access to, and use of, recorded material.

3.5 A Storage Device Release form will be completed before any storage device is disclosed to appropriate authorities. The form will indicate who took the device, under what authority, when this occurred, and if it will be returned or destroyed after use.

4.0 Retention

4.1 When covert recorded information has been viewed the retention period shall be the longer of one year from the date of viewing or for one year from the date of resolution of the Education Act incident in accordance with Section 5 of Ontario Regulation 823 under *MFIPPA*.

2.1 APPENDIX A

DEFINITIONS

Authorized Personnel - individuals authorized by the Director of Education/designate and/or the school principal to use video surveillance equipment or view tapes

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. If a video surveillance system displays these characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered "personal information" as defined under the *Municipal Freedom of information and Protection of Privacy Act*.

Record - any record of information, however recorded, whether in printed form, 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.

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 (including streets, highways, parks). The term video surveillance system includes an audio device, thermal imaging technology or any other component associated with capturing the image of an individual.

Reception Equipment - 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.

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

Covert Surveillance - surveillance conducted by means of hidden devices, without notice to the individuals being monitored

Thames Valley
District School Board

~~3.1 APPENDIX B~~

~~SAMPLE OF NOTICE TO PARENTS/GUARDIANS/ADULT STUDENTS~~

~~Dear Parent/Legal Guardian/Adult Student:~~

~~We make every effort to provide a safe and welcoming learning environment for our students and staff. To this end and after careful consideration, it has been determined that a video surveillance program is necessary to enhance safety and deter vandalism. In the coming weeks, a surveillance system will be installed and monitored in accordance with Board Policy and Procedures and~~compliance with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). For additional information please contact the Principal/Supervisor of this site.

Contact information is available in the office/front desk or visit our website – www.tvdsb.ca

~~Video equipment will be located, for example, in public areas of the school or at the front of school buses serving the school and will be clearly identified with appropriate signage.~~

~~The equipment will not be located in areas where there is an expectation of privacy such as washrooms or change rooms. Access to the equipment will be restricted to authorized personnel only – school and Board administration and, where necessary, police conducting an investigation.~~

~~We feel this is an important step in maintaining a safe and secure learning environment for our school community. If you have any questions or concerns in this regard, please contact me to discuss them.~~

~~Sincerely,~~

~~Principal~~.