

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, 2025 June 06
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.