

Tracking and Surveillance

Procedure 228

Revised: 9/2/2026

Statement

Tri-Board Student Transportation Services authorizes the use of tracking and surveillance technology on school buses to promote student safety and efficiency of service. In the event of a reported or observed incident, this technology may be used to assist in the investigation of the incident.

All Bus Operators are contractually obligated to have working Automatic Vehicle Locators (AVLs) and video cameras installed on all school buses/vans servicing Tri-Board.

Tracking and surveillance technology are used on school buses in accordance with the [Highway Traffic Act](#) (HTA), the [Municipal Freedom of Information and Protection of Privacy Act](#) (MFIPPA), and The Information and Privacy Commissioner of Ontario's (IPC) [Guidelines for the Use of Video Surveillance](#) principles.

Procedure

Automatic Vehicle Locator (AVL)

Data collected through AVLs is used by Tri-Board and the Operator to track route schedules, vehicle speeds and stop locations, ensure route efficiencies, and use of equipment required under the HTA. Only the Operator and Tri-Board can view this information. Live AVL data cannot be accessed by families or school administration.

Video Surveillance

Each Operator contracted with Tri-Board is responsible for procuring and maintaining the camera systems used on their buses. Cameras will be installed to view the interior of the vehicle where students will board and be seated.

Responsibilities of Bus Operators

The Operator is responsible for the video surveillance system on the bus/van and will:

- a) ensure it is properly installed;
- b) ensure surveillance notice decals are on the outside of the bus
- c) check the surveillance system periodically to ensure it is in working order;
- d) maintain control of the surveillance system at all times;
- e) ensure that the privacy and confidentiality of information collected is preserved;
- f) be familiar with this procedure;
- g) be aware of MFIPPA and the requirement to protect personal information and keep it
- h) confidential;

- i) ensure that only authorized personnel use the system, and are aware of their obligations under MFIPPA and this procedure;
- j) report any potential breaches of information to Tri-Board and follow direction from Tri-Board

Responsibilities of Tri-Board

- a) respond to requests for access
- b) ensure Operator compliance
- c) respond to possible breaches, working with the Operator to investigate

Notice of Surveillance

Signs will be posted on the bus providing notice to the public of the presence of video cameras. One sign will be posted on the outside of the bus, and one will be posted inside the bus as part of the “School Bus Rules”.

A notice is posted in the Student Portal, where families access their student’s transportation information after applying, identifying the use and purpose of video surveillance.

Access to Footage and Storage

Only the Operator and Tri-Board Management will have access to recorded video.

Recorded video will be reviewed as the need arises. Circumstances that warrant a review should be limited to instances where an incident has been reported or observed in order to protect the safety of students, drivers, or monitors.

Live footage will only be viewed when there is an imminent risk to students. Circumstances that warrant a viewing should be limited to:

- a) If the bus/van has been involved in a significant incident/accident/collision
- b) A student is reported missing

Recorded video may be reviewed by other authorized personnel, in accordance with MFIPPA, where a serious or violent incident has been reported/observed or to investigate a potential crime.

Retention

Retention periods vary by supplier. Camera footage is stored in a cloud-based system. Depending on the supplier, footage is accessible for 2-4 weeks and then is recorded over. Saved footage is accessible from the cloud for approximately 3 months.

Recorded video used as part of an investigation or disciplinary action must be retained for a minimum of one year, or one year from the date of resolution of the incident, whichever is longer.

Access Requests

Access and review of recorded video will be tracked through Tri-Board’s **School Bus Camera Footage Request** form, to provide an audit trail and for future reference. This form must be completed when viewing or storing recorded video that is being used as part of an investigation or disciplinary action, and when releasing any recorded video to police or other entities authorized under MFIPPA.

School Administrators may request to view recordings where an incident has been reported or observed in order to protect the safety of students, drivers, or monitors. Tri-Board will review the

request based on this procedure. A parent/guardian, student or individual has the right to make a request to view personal information contained on recorded video relevant to them, subject to the provisions of MFIPPA. Responses to access requests must be provided in consultation with the freedom of information coordinator and/or school superintendent, in accordance with MFIPPA, Section 36 (1) and Section 38, to ensure the privacy and protection of others.

Privacy Breach

Should an incident occur involving inadvertent or unauthorized disclosure or inappropriate use of personal information contained on recorded video media, immediate steps must be taken to assist in the containment of a privacy breach and mitigate risks. In the event of a breach or potential breach, the following steps will be taken:

1. The Operator will assess the situation to determine if a breach or potential breach has indeed occurred and contact Tri-Board.
2. Tri-Board will report the privacy breach to key persons at the applicable school board(s) and, if necessary, to law enforcement.
3. The Operator and Tri-Board will identify the scope of the breach and contain it. Containment involves taking immediate action to put an end to the unauthorized access, where possible. For example:
 - a. retrieving hard copies of any personal information that has been disclosed,
 - b. revoking or changing passwords and identification numbers,
 - c. temporarily shutting down the system/ device,
 - d. correcting weakness in physical or electronic security.
4. Tri-Board will document the breach and containment activities and develop briefing materials.
5. Tri-Board will brief key persons on the privacy breach and how it is being managed.
6. Once the privacy breach is confirmed and contained, Tri-Board and the Operator will conduct an investigation to determine the cause and extent of the breach.
 - a. Identify and analyze the events that led to the privacy breach.
 - b. Evaluate if it was an isolated incident or if there is a risk of further exposure of information.
 - c. Determine who was affected by the breach (e.g. students or employees), and how many were affected.
 - d. Evaluate the effect of containment activities.
 - e. Evaluate who had access to the information.
 - f. Evaluate if information was lost or stolen.
 - g. Evaluate if information has been recovered.
7. Tri-Board shall consult with the applicable school board(s) to determine what notifications are required. Considerations may include notification to the affected individual and authorities and organizations such as police, the Information and Privacy Commissioner, financial institutions or other parties that may be affected; other departments and employees; unions or employee groups and the board members. In determining if notification is required to the affected individual(s) the following shall be considered.
 - a. Who had access to the breached personal information?
 - b. Does the loss of theft place an individual at risk of physical harm?
 - c. Is there a risk of identity theft or other fraud?
 - d. Is there a risk of hurt, humiliation or damage to reputation?
8. Notification should be done promptly, and shall include:
 - a. a description of the incident and the information involved;

- b. the nature of potential or actual risks or harm;
 - c. what mitigating actions the board is taking;
 - d. appropriate action for individuals to take to protect themselves against harm;
 - e. a contact person for questions or to provide further information; and
 - f. contact for the Information Privacy Commissioner, if the office of the Information and Privacy Commissioner (IPC) is investigating. Include an explanation of the individual's right to complain to the IPC.
9. Tri-Board will determine what changes and remedial actions need to be implemented, consider whether it is necessary to:
- a. review the relevant information management systems to enhance compliance with privacy legislation;
 - b. amend or reinforce the existing policies, procedures, and practices for managing and safeguarding personal information;
 - c. develop and implement new security or privacy measures, if required;
 - d. review employee training/awareness on legislative requirements, security and privacy procedures and practices to reduce potential or future breaches, and strengthen as required;
 - e. test and evaluate remedial actions to determine if they have been implemented correctly and if policies, procedures, and practices need to be modified; and/or
 - f. recommend remedial action to the CEO.