



CAMERA SURVEILLANCE GUIDELINES

Preamble: These guidelines are in accord with Cambridge Middle School **Property Management Policy** as approved by the School Board in **August 2022**. The school's camera surveillance system is installed to deter crime and undesirable behaviours, and provides greater protection for our students and staff, and prevents less wilful damage to property. The system operates 24 hours a day, seven days a week.

The school complies with the Privacy Act (2020) in using and managing the system and every effort is made to prevent it impacting on the privacy of the school community in its daily life. Specifically, the Privacy Act 2020 demands that:

- Information is only collected for a necessary and lawful purpose.
- Individuals must be aware of the information collection and the reason for it.
- Information collected for one purpose cannot be used for another.
- Information is stored and disposed of securely.

Guidelines:

1. The school's Principal is responsible for overseeing the CCTV system.
2. The system is installed so that individuals committing a crime on school grounds can be identified and if necessary, prosecuted. It is only used to identify persons illegally on the premises or engaged in criminal activity, or any persons disturbing the normal operations of the school.
3. Access is limited to the Principal and appointed system managers. A google doc is used which details access to the system, the purpose of the access, and the operator.
4. Staff are advised that while they go about their normal business at the school, their recorded images, and those of their students, will not be reviewed except to identify culprits.
5. No recorded data is taken from the system unless approved in writing by the Principal.
6. Police may request access to CCTV records when investigating criminal activity in the area. The police are given access to the system as required but must comply with these guidelines. If the school has concerns about releasing this information, it will contact appropriate legal advisors. The school must comply if the police have a search warrant.
7. Requests for access to the system from parents or other interested parties will be denied unless good cause is given and the school board formally approves this access.
8. Any system misuse is reported to the principal, or the school board if the principal is involved.
9. The school has signage in strategic places to inform people of the system, and the reason for it.
10. Staff have the right to see footage of themselves as it is personal information held about them. However, they can only see such footage if it is readily retrievable. Staff are required to supply a time, date and location. The privacy of other people who may be in the footage must be considered in such a case.

11. All data, hard drives, etc., are destroyed or stored in compliance with the approved standard on data protection. Data is stored according to the standard so that it is not compromised and can be successfully used in court as evidence.
12. Cameras are not installed in sensitive places such as bathrooms.
13. The school's monitoring firm provides regular reports on the effectiveness of the system, and the system's operation is checked regularly by the privacy officer and monitoring firm.
14. The system, its operation, and related policies and procedures are audited and evaluated regularly as part of the annual health and safety audit.

Review: 2025

These Guidelines will be reviewed in accord with the review of the school's Property Management Policy