

Administrative Procedure 175

General Administration

VIDEO SURVEILLANCE AND SECURITY CAMERAS

BACKGROUND

Westmount Charter School (WCS) is committed to maintaining a safe and caring environment while protecting the privacy of students, employees, families, volunteers, visitors, and members of the public.

Video surveillance and video-enabled entrance systems may be used at WCS facilities where they serve a reasonable and necessary safety, security, property protection, building access, or operational purpose. Its use must be balanced with individuals' reasonable expectations of privacy and limited to what is necessary to achieve the authorized purpose.

Video surveillance may constitute the collection of personal information when it records an identifiable individual. WCS will collect, use, disclose, retain, protect, and dispose of surveillance information in accordance with the *Protection of Privacy Act* (POPA), *Access to Information Act* (ATIA), WCS's Privacy Management Plan (PMP), and related Administrative Procedures.

Video surveillance supports, but does not replace, appropriate supervision, building security, emergency procedures, and other measures used to maintain safe and caring school environments.

DEFINITION

Audio Intercom	The two-way audio functionality associated with a WCS entrance or building access system that enables authorized personnel to communicate with individuals requesting access to a WCS facility.
Authorized Personnel	Employees specifically authorized by the Superintendent or designate to access, review, administer, or maintain video surveillance systems or recordings.
Personal Information	Recorded information about an identifiable individual, as defined by POPA.
Recording	Video, images, or authorized audio captured and retained by a WCS surveillance or entrance intercom system.
Video Surveillance	The use of cameras or related technology to observe and/or record activities occurring on or around WCS property for an authorized purpose.

PROCEDURES

1. Authorization and Purpose
 - 1.1 Video surveillance systems may be installed and operated on WCS property where the Superintendent determines that there is a reasonable and necessary safety, security, property protection, building access, or operational purpose.
 - 1.2 Video surveillance will only be used for authorized purposes, which may include:

- 1.2.1 Promoting the safety and security of students, staff, volunteers, visitors, and WCS facilities;
 - 1.2.2 Facilitating safe and controlled access to WCS facilities;
 - 1.2.3 Deterring or investigating unauthorized access, vandalism, theft, property damage, or other security incidents;
 - 1.2.4 Supporting the investigation of significant safety, security, or behavioural incidents where reviewing recorded information is reasonably necessary; and
 - 1.2.5 Supporting emergency response or other legitimate operational requirements.
 - 1.3 Surveillance will not be used routinely for monitoring employee performance, instructional practice, or student behaviour where there is no reasonable safety, security, investigative, or other authorized purpose.
 - 1.4 Before implementing a new video surveillance system or making a substantial change to an existing system, WCS will assess the privacy implications and complete a Privacy Impact Assessment (PIA) where required by POPA, applicable regulations, and AP-171 Privacy Impact Assessments.
 - 1.5 WCS will limit the collection of personal information through surveillance and entrance intercom systems to that which is reasonably necessary to achieve the authorized purpose.
2. Camera Placement
- 2.1 Cameras will be positioned only in locations reasonably necessary to achieve the identified purpose.
 - 2.2 Cameras may be located in areas such as:
 - 2.2.1 Building entrances and exits;
 - 2.2.2 Hallways and common areas;
 - 2.2.3 Parking areas;
 - 2.2.4 Exterior grounds;
 - 2.2.5 Building perimeters; and
 - 2.2.6 Other areas identified through safety or security assessment.
 - 2.3 Camera positioning and field of view will be limited, where reasonably possible, to the area necessary to achieve the authorized purpose.
 - 2.4 Video surveillance will not be installed in areas where individuals have a heightened reasonable expectation of privacy, including washrooms, change rooms, counselling rooms, or other similarly private spaces.
 - 2.5 WCS entrance and building access systems may include two-way audio functionality to enable authorized personnel to communicate with individuals requesting access to a WCS facility. Audio functionality will be limited to active intercom communications. Continuous audio monitoring or recording outside of an active intercom communication will not be enabled. Where audio is retained in connection with an intercom communication, it will be subject to the access, use, disclosure, security, retention, and disposal requirements of this Administrative Procedure.
3. Notification and Collection Notice
- 3.1 WCS will provide reasonable notice that video surveillance is in use and, where applicable, that audio may be collected through an entrance intercom system.

- 3.2 Appropriate signage and/or collection notice will be displayed at entrances to WCS property and/or in areas subject to surveillance.
- 4. Access to Recordings
 - 4.1 Access to video surveillance systems and recordings will be limited to authorized personnel with a legitimate need to access the information.
 - 4.2 Recordings may be reviewed by the Superintendent, Principal, or other authorized personnel where reasonably required for an authorized purpose under this procedure.
 - 4.3 IT personnel may access surveillance systems where necessary for system administration, maintenance, security, or technical support but will not routinely review recordings unless authorized.
 - 4.4 Access credentials must not be shared with unauthorized individuals.
 - 4.5 Access to surveillance systems and recordings will be logged or otherwise auditable, where supported by the surveillance system.
- 5. Use and Disclosure
 - 5.1 Recordings will only be used for the purpose for which the information was collected or as otherwise authorized or required by law.
 - 5.2 Recordings will not be copied, downloaded, photographed, transmitted, or shared except where necessary for an authorized purpose.
 - 5.3 WCS may disclose surveillance recordings where authorized or required by law, including, where appropriate, to:
 - 5.3.1 Law enforcement;
 - 5.3.2 Emergency responders;
 - 5.3.3 Legal counsel;
 - 5.3.4 Regulatory or investigative bodies; or
 - 5.3.5 Another person or organization where disclosure is legally authorized.
 - 5.4 Requests from law enforcement or other external parties for surveillance recordings will be referred to the Superintendent and/or WCS Access and Privacy Officer, as appropriate, before disclosure, except where disclosure is otherwise authorized or required by law.
 - 5.5 Any disclosure will be limited to information reasonably necessary for the authorized purpose.
- 6. Retention and Disposal
 - 6.1 Recordings will be retained only for as long as necessary to fulfill the authorized purpose and in accordance with AP-180 Records Retention and Disposition and WCS's approved records retention schedule.
 - 6.2 Recordings not required for an investigation, legal proceeding, access request, insurance matter, or other authorized purpose will be securely overwritten or destroyed according to the established retention schedule.
 - 6.3 Where a recording becomes relevant to an investigation, complaint, legal proceeding, access request, or other matter, it will be preserved until the matter and any applicable retention requirements are concluded.
- 7. Security
 - 7.1 WCS will implement reasonable administrative, technical, and physical safeguards to protect surveillance systems and recordings against unauthorized access, collection, use, disclosure, copying, modification, loss, or destruction.

- 7.2 Surveillance systems will be appropriately secured through measures such as access controls, passwords, account management, secure storage, system updates, and other safeguards appropriate to the technology.
 - 7.3 Any actual or suspected unauthorized access, collection, use, disclosure, loss, or destruction of surveillance information must be reported immediately in accordance with the WCS Privacy Management Program (PMP) and applicable privacy incident response procedures.
8. Access Requests
- 8.1 Requests from individuals seeking access to surveillance recordings containing their personal information will be managed in accordance with ATIA, POPA, and applicable WCS access and privacy procedures.
 - 8.2 Access to a recording may require redaction, masking, blurring, or other measures to protect the personal information and privacy rights of other individuals.
 - 8.3 Staff receiving a formal request for surveillance footage will forward the request to the Access and Privacy Officer and will not independently release the recording.
9. Prohibited Uses
- 9.1 WCS surveillance systems and recordings must not be:
 - 9.1.1 Accessed out of curiosity or for personal purposes;
 - 9.1.2 Used to monitor individuals without an authorized purpose;
 - 9.1.3 Shared through personal email, messaging applications, social media, or unauthorized devices;
 - 9.1.4 Recorded using a personal device or otherwise reproduced without authorization; or
 - 9.1.5 Disclosed to students, parents, employees, or other individuals except through an authorized process.
 - 9.2 Unauthorized access, use, copying, or disclosure may constitute a privacy incident and may result in disciplinary or other appropriate action.
10. Roles and Responsibilities
- 10.1 The Superintendent is responsible for:
 - 10.1.1 Approving the installation and significant expansion of video surveillance systems;
 - 10.1.2 Ensuring surveillance practices comply with legislation and WCS procedures;
 - 10.1.3 Authorizing appropriate access; and
 - 10.1.4 Overseeing significant requests, investigations, or disclosures.
 - 10.2 The Access and Privacy Officer is responsible for:
 - 10.2.1 Providing privacy advice regarding surveillance;
 - 10.2.2 Determining when a PIA or other privacy assessment is required;
 - 10.2.3 Supporting access and disclosure decisions;
 - 10.2.4 Responding to privacy incidents; and
 - 10.2.5 Ensuring alignment with the WCS Privacy Management Program (PMP).

- 10.3 The Principal is responsible for ensuring surveillance systems at their campuses are used in accordance with this Administrative Procedure and for referring privacy, access, and disclosure matters appropriately.
- 10.4 Information Technology (IT) is responsible for the technical administration, security, maintenance, access controls, and integrity of the WCS surveillance system.

Legal Reference:	<i>Education Act</i> <i>Protection of Privacy Act (POPA)</i> <i>Access to Information Act (ATIA)</i>
Cross Reference	AP-171 Privacy Impact Assessments AP-180 Records Retention and Disposition
Date of Adoption:	August 28, 2026
Date of Revision:	
Due for Review:	August 28, 2029