

MAS Security Camera Policy



I. PURPOSE

The Governing Council authorizes the use of video safety and security technology at MAS campuses, including sports fields, parking lots and designated areas within buildings. Some school transportation may also have this technology. The primary reasons MAS uses safety and security technology (a camera and monitoring system) are as follows:

- To promote and foster a safe and secure teaching, learning, and working environment for students, staff, and visitors.
- To deter, prevent, and assist in the investigation of student misconduct, unauthorized campus entry, theft, vandalism, and other criminal activity.
- To protect MAS facilities, and property.
- To formalize procedures handling, viewing, retention, dissemination, and destruction of surveillance records.

II. SCOPE

This policy applies to all students, staff, volunteers, contractors, and visitors on school grounds, inside school buildings, at school-sponsored events, and within MAS vehicles (including school buses where applicable). Video-only security cameras may be installed in situations or places (both outside and indoors) where security and safety of person or property would be enhanced. However, cameras will be limited to uses that do not violate the reasonable expectation of privacy

This policy does not apply to:

- Video or audio recordings captured during public events (*e.g., athletic events, theatrical performances, public board meetings*).
- Technology utilized for distance learning, online instruction, or authorized classroom-based instructional activities.
- Video recordings utilized solely for the purpose of licensed educator performance evaluations or personnel policies.

III. CAMERA PLACEMENT AND PROTECTION OF PRIVACY

MAS respects acknowledges that students, staff, and community members have a reasonable, but limited expectation of privacy while at school and work.

A. Permitted Locations

Security cameras may be installed in visible, public, or common-use areas where there is no reasonable expectation of privacy. Authorized locations include:

- Building perimeters, main entryways, and exits.
- Parking lots, athletic fields, playgrounds, and exterior school grounds.
- Hallways, stairwells, foyers, and lobbies.
- Large gathering spaces, such as cafeterias, gymnasiums, and libraries.
- Student transportation vehicles (buses).

B. Prohibited Locations (Protected Privacy Zones)

Information obtained from security cameras shall be used for safety and security purposes

continued

and for law and policy enforcement, including, where appropriate, student judicial functions (e.g., *student disciplinary hearings*). Security cameras will not be installed or directed to record inside areas where individuals have a well-defined expectation of privacy, including:

- Restrooms, locker rooms, and changing areas.
- Staff break rooms or private offices.

All video camera installations will be visible to students and staff and may be located in hallways, stairwells, large group meeting areas and outside the school buildings.

C. Classroom Recording

Cameras shall not be placed inside classrooms for general, routine monitoring unless specifically authorized by the CEO for documented safety or security needs. However, classroom recordings may, with prior notice to the teacher, be used for professional development and support of teacher improvement.

D. Audio Recording

Unless explicitly permitted under state law and specifically authorized by the Governing Councils, security cameras shall record **video only**. Audio recordings are strictly prohibited.

IV. NOTICE AND SIGNAGE

MAS will provide clear and conspicuous notice regarding the use of video surveillance:

A. Physical Signs:

MAS will post signs in all primary building entrances and in other visible public areas noting the use of safety and security cameras.

B. Written Notification:

MAS will post signs in all primary building entrances and in other visible public areas noting the use of safety and security cameras.

C. Vehicle Notice:

Signs will be posted inside all MAS vehicles (including buses) if equipped with surveillance systems.

V. ACCESS AND MONITORING

A. Controlled Access:

Only the CEO and administrative/security personnel who have a legitimate educational or operational need to perform their duties shall have access to live camera feeds or recorded footage.

B. Technical Staff Access:

IT and systems administration staff may access the platform solely for system maintenance, network troubleshooting, and security administration, but shall not review or export footage unless authorized in writing by the CEO or authorized administrative personnel.

C. Screen Privacy:

Security monitors displaying live feeds are located in controlled-access areas (e.g., *administrative offices*) and positioned so that the general public, students, and unauthorized staff cannot view them.

continued

VI. DATA RETENTION AND SECURITY

A. Routine Storage:

Recorded footage shall be stored on secure, access-controlled servers or encrypted cloud systems. Routine footage will be automatically overwritten after ninety (90) days unless a specific clip is extracted and preserved. No individual shall store or hold video surveillance recordings in their possession.

B. Investigation Holds:

If a recording contains evidence of an active safety incident, student disciplinary infraction, staff misconduct, or potential criminal behavior, it shall be extracted and preserved securely in its original format. This preserved footage will be kept until the resolution of the administrative or legal proceeding, or in accordance with state public records retention schedules.

C. Logs:

A log shall be maintained of all instances of access to or use of surveillance records. The record shall include the date and name of the person or persons accessing the recordings.

D. Tampering Prohibited:

No student, staff member, or unauthorized individual may alter, disable, delete, or tamper with any security camera or video recording. Violations will result in disciplinary action up to and including termination or expulsion, and referral to law enforcement.

VII. STUDENT RECORDS AND DISCLOSURE (FERPA COMPLIANCE)

A. Viewing Requests by Parents/Eligible Students:

A parent or eligible student (18 years or older) has the right to inspect and review security camera footage that is directly related to them or their child.

- If the footage involves other students, MAS will comply with FERPA. Generally, a parent may view the video if their child's actions cannot be separated from the actions of other students, provided it does not violate the confidentiality of those other students' disciplinary outcomes.
- Digital redaction (such as blurring faces of uninvolved peers) may be utilized if feasible prior to disclosure but is not strictly required for a visual review if it would destroy the context of the incident.
- With certain exceptions, MAS is not required to provide a copy of the surveillance recording maintained as an education record under FERPA.

B. Third-Party Disclosures:

MAS will not release security camera footage containing student education records to third parties without the prior written consent of the parent/eligible student, except as permitted under FERPA exceptions (*e.g., to law enforcement in a health or safety emergency, or pursuant to a lawfully issued subpoena or court order*).

VIII. COLLABORATION WITH LAW ENFORCEMENT

A. Active Emergencies:

During an active crisis, natural disaster, or immediate threat to life and safety, live camera feeds may be shared in real-time with emergency responders and law enforcement.

continued

B. Routine Investigations:

Law enforcement requests for recorded footage must be submitted in writing to the School Leader. The School Leader should consult with legal counsel prior to disclosing the information.

C. Log of Disclosure:

MAS will maintain a secure log of all external requests, reviews, and releases of security camera footage, documenting the date, requesting party, purpose, and authorizing administrator.

IX. VIOLATIONS AND SANCTIONS

Any employee or student who violates this policy, including unauthorized viewing, copying, or distributing of footage, or tampering with equipment, shall be subject to disciplinary action under applicable MAS policies, up to and including termination of employment, expulsion, and/or referral to civil or law enforcement authorities.

Adopted on: August 20, 2026

Last Reviewed/Revised: August 20, 2026