



RED ROCKS COMMUNITY C O L L E G E

Security Camera Update Frequently Asked Questions (FAQ)

August 12, 2026

Quick Facts

- Security camera footage is stored on RRCC's on-premises servers, not in the cloud.
- Recorded footage is retained for 30 days and then automatically deleted unless needed for an active investigation, legal hold, or authorized purpose.
- Access to footage is limited to the campus police department, and the security camera vendor is contractually prohibited from accessing RRCC footage or servers.
- AI features are not enabled because RRCC has not licensed the software needed to use them.
- RRCC does not proactively share security camera footage with federal, state, or local agencies. Requests for footage require appropriate legal authority and review.

How does Red Rocks Community College use security cameras?

Red Rocks Community College has long used security cameras as one of the multiple strategies to protect the entire community. Specifically, security cameras support campus safety, security, investigations, and operational needs. Cameras help deter crime, monitor college property, assist in the response to, and investigation of incidents, support law enforcement, and emergency response activities, and provide video evidence when incidents occur.

The camera system is not continuously monitored by personnel. Cameras are primarily used to record and preserve footage for later review when needed.

Who Can See the Footage and How Is It Protected?

Where is the security camera footage stored?

Recorded footage is stored on the college's on-premises servers. The camera footage is not uploaded to the cloud or shared with third parties absent a valid legal request for the information.

How long is the security camera footage retained?

Recorded footage is stored on the college's on-premises servers for 30 days. After the retention period expires, footage is automatically deleted unless it has been preserved for an active investigation, evidentiary purposes, litigation hold, or other authorized operational or legal purpose.

Could the manufacturer of security cameras or other third parties access the footage without RRCC's permission?

RRCC has taken every practical step to ensure that no third parties can access footage from security cameras without authorization. Mitigation measures include:

- The security footage is being housed on our local servers and not in the cloud.
- The servers are in secured rooms.
- Permissions to access footage on the servers are limited to the campus police department.
- Per the contract terms and conditions with Motorola, the camera manufacturer may not access our footage or servers.

Does RRCC share security camera footage with third parties or other state, federal or local agencies?

We have heard concerns about whether camera footage could be shared with immigration enforcement or other outside agencies. RRCC does not proactively share security camera footage with any federal, state, or local agency. Absent a valid subpoena, FERPA release, or open records request, every request gets case-by-case legal review, and disclosure is a rare exception. RRCC also does not share security camera footage with any third party.

Are there AI features on the cameras and are the AI features currently being used?

Many modern security cameras include AI-capable features as part of the standard hardware platform, including the equipment purchased by RRCC. However, RRCC has elected to not license the software necessary to utilize the AI capabilities - including facial recognition, automated tracking, weapon detection, and behavioral analytics. AI features are not currently enabled on the college's camera system.

What would be required to enable the AI features?

Enabling AI functions would require additional software licensing and configuration through the camera system vendor.

Who would approve the use of AI features with security cameras in the future?

Any decision to enable such features would be subject to institutional review, applicable laws, and policies, vetting by the Chief of the Campus Police Department and approval by the College President.

Your Privacy

What are reasonable privacy expectations when it comes to the use of security cameras?

Security cameras are generally considered appropriate in public or common areas where individuals do not have a reasonable expectation of privacy, such as:

- Parking lots
- Building entrances and exits
- Transactional spaces such as the cashier's office, cafeteria, IT helpdesk, etc.
- Hallways, lobbies, and front desk spaces
- Exterior Public Spaces
- Interior common or publicly available spaces

Security cameras are not installed in the following areas:

- Restrooms
- Locker Rooms/ Changing Areas
- Individual Offices
- Medical Offices/Counseling Centers
- Classrooms

How are security cameras used for surveillance?

The security cameras are used by campus police personnel when they become aware of an incident, either in real time or after the fact. As a general rule, security cameras are used for passive surveillance.

Security, Compliance, and Legal Requirements

Why were new security cameras purchased?

There are three reasons the college is updating security cameras.

First, the previous camera system had reached the end of its supported lifecycle. As technology ages, manufacturers eventually discontinue software updates, security patches, and technical support for older hardware and software platforms.

Second, the firmware for the legacy security cameras was vulnerable to cyber-attacks. Upgrading the camera system helps ensure continued compatibility with the college's technology infrastructure and allows the system to receive current security updates and manufacturer support. Maintaining supported technology is a vital component of the college's overall cybersecurity and risk management practices.

Third, the legacy cameras were not providing sufficient physical coverage to meet the security, safety, and investigative needs of the campus.

What were the cybersecurity considerations in replacing security cameras?

Upgrading the camera system helps ensure continued compatibility with the college's technology infrastructure and allows the system to receive current security updates and manufacturer support. Maintaining supported technology is a vital component of the college's overall cybersecurity and risk management practices.

What laws and regulations govern security camera use at higher education institutions?

There is no single federal law that comprehensively regulates security camera use at colleges and universities. Institutions must comply with applicable federal and state laws that govern protection of information including privacy protections and constitutional requirements where applicable.

The Colorado Community College System Procedure SP19-50 expressly permits "video recording and photographing of System buildings, individuals, and events taking place in areas open to the public, ... provided it does not interfere with official System business or endanger the safety of others."

Some examples of legal and policy implications that impact how security camera footage is shared include:

Student Privacy

In some circumstances, video footage may be considered personally identifiable information or an education record under the Family Educational Rights and Privacy Act (FERPA) if it is directly related to a student and maintained by the institution. When either circumstance applies, access to and disclosure of the footage may only be provided in accordance with federal law, such as with permission of the student or pursuant to a subpoena or court order.

Employee and Academic Considerations

The use of cameras in classrooms and workspaces may be subject to additional legal, contractual, policy, or academic considerations. Any use of cameras in instructional environments must comply with applicable laws, institutional policies, and collective bargaining agreements, if applicable.

Public Records Requests

Surveillance footage may be requested by the public under the Colorado Open Records Act and/or the Colorado Criminal Justice Records Act.

Requests for footage are reviewed on a case-by-case basis. The release of footage may be subject to applicable legal restrictions, privacy considerations, investigative concerns, and required redactions. Depending on the circumstances, footage may be released in full, released in a redacted format, or withheld as permitted by law.

For example, footage may be exempt from public disclosure if it reveals "specialized details of security arrangements", library lending information, FERPA protected student education records, HIPAA protected personally identifiable information or is part of an active or pending law enforcement investigation.

Project Logistics

Are both the Lakewood and Arvada campuses included in the security camera upgrade project?

Yes. Both the Lakewood and Arvada Campuses are included in the project and are receiving upgraded cameras to replace the existing end-of-life camera system.

What are the phases of the college's security camera project?

The camera project is being implemented in three phases:

Phase 1: Replace existing end-of-life cameras at both Lakewood and Arvada Campuses. This phase also includes the installation of a limited number of additional cameras to address identified coverage gaps. Phase 1 was completed over the summer of 2026.

Phase 2: Evaluate and address any remaining coverage gaps on either campus.

Phase 3: Expand camera coverage in parking lots and increase exterior camera coverage at both the Lakewood and Arvada Campuses.

Are the security cameras connected to the college's Wi-Fi?

No. The security camera system in the buildings is hardwired and do not rely on Wi-Fi for connectivity.

What brand of security cameras is the college installing?

The college has historically utilized cameras manufactured by Avigilon. The current security camera upgrade project continues with the use of Avigilon camera systems, a Motorola Solutions company. Motorola Solutions is a state partner. Keeping the same platform for our security cameras saved time, money, and effort.

Is the College comfortable with Avigilon or Motorola as vendor for this project?

Yes. Avigilon was our prior security camera vendor and is a state vendor that has been used without incident by our fellow CCCS schools and other state agencies.

Furthermore, Avigilon does not have access to the footage produced by the security cameras - the footage is stored on RRCC's local servers, access is limited to Campus Police, Avigilon is contractually prohibited from accessing RRCC footage or servers, and RRCC does not proactively share footage with outside agencies.

How did the college pay for security cameras?

The college is using reserves to pay for security cameras.

Timing of Communications

The camera project was a replacement of an existing security camera system that had reached the end of its supported life cycle and presented cybersecurity and operational concerns. Planning started in 2023 as part of the college's facilities, technology, and public safety processes. As installation began in 2025, additional student and

community questions emerged, and the college spoke to various constituency groups and developed this comprehensive FAQ to provide broader information about the project and address community concerns.