

UCR Policies and Procedures

Policy Title: **Campus Camera Systems**

Policy Number: 850-44

Responsible Officer:	Chief of Police
Responsible Office:	The UC Riverside Police Department (UCPD)
Origination Date:	[], 2026
Date of Revision:	First version
Date of Last Review:	[]/[]/2026

I. Policy Summary and Scope

The University of California, Riverside (UCR) is committed to enhancing the quality of life for the campus community by integrating best practices in safety and security with technology. In support of UC Privacy Principles, the UCR Principles of Community, and applicable state and federal laws, this policy addresses the use of campus cameras while strictly respecting and preserving individual privacy rights.

This policy:

- Regulates the use of cameras—including open space camera systems used to observe public areas—on property owned, operated, leased, or maintained by UCR, including University vehicles.
- Establishes processes for requesting new cameras and updating and maintaining existing systems.
- Includes protocols for the recording, handling, viewing, retention, dissemination, and destruction of digitized camera records.

Included in Scope:

Fixed cameras, including those monitoring high-traffic areas, property protection systems, and any other cameras on University Property not explicitly excluded from this policy's scope. All cameras installed prior to the issuance of this policy are also subject to the standards and requirements set forth herein.

Excluded from Scope:

- Any covert camera systems or any other camera devices used by UCPD, including body-worn cameras and UCPD drone video (Reference section V.B.)
- Course instruction, academic or lab research, or creative works (e.g., Classroom/Test Center cameras).
- Video conferencing tools (e.g., Zoom, Microsoft Teams) used for meetings.
- Systems used in healthcare or clinical settings that may capture Protected Health Information (PHI) (governed by applicable laws, including HIPAA, and University healthcare privacy and

UCR Policies and Procedures

security policies).

- Personal cameras used for non-University purposes, except as provided under Section III.A.3 below.
- Automated License Plate Readers (ALPR) used by UCR Transportation and Parking Services.
- Photography used for evidentiary purposes in Parking operations.
- Commercial Use Production (UCR policy - Campus Filming 700-15).
- Cameras used for broadcasting or recording public campus events (e.g., athletics, commencement ceremonies, theatrical performances).
- Unmanned Aircraft Systems (UC Unmanned Aircraft System (Drone) Policy).
- Construction cameras operated by third-party contractors.

II. Definitions

- **Camera:** Devices that capture still or moving images, photos, video recordings and/or audio on University Property.
- **Camera Governance Group:** An administrative oversight body that informs and advises on the strategic direction, policy compliance, funding recommendations, and maintenance prioritization of the campus cameras.
- **Designated Campus Authority:** The Chief of Police and the Chief Information Officer, or designees, are responsible for approving and overseeing camera systems.
- **Operator:** Any authorized individual with access to Video Data (VD).
- **Preservation (Preserved):** The process of securely retaining Video Data (VD) to prevent deletion or loss for legal, investigative, or administrative purposes.
- **System:** A system, or camera system, is defined as an integrated, modular network of hardware and software components standardized to capture, process, monitor, and manage visual and associated audio data across multiple applications.
- **University Property:** Property owned, operated, leased, or maintained by UCR, including University vehicles.
- **Video Data (VD)** – Visual images recorded by University Cameras and/or Systems that can be replayed, stored, and deleted.

III. Policy

As detailed in this policy, all camera installations, modifications, and removals require formal approval prior to implementation. Access to recorded video data is strictly restricted and granted solely upon authorization from the UC Riverside Police Department (UCPD) (Sections III.A.1 and III.E.1) or as otherwise required by state and federal law. To maintain a standardized footprint, UCR integrates approved safety cameras into new construction and major renovation projects where appropriate (Section III.A.2). The comprehensive approval process strictly respects established privacy principles and ethical standards (Section III.B), governed by an oversight group to ensure continuous institutional accountability (Section III.C). Additionally, Information Technology Solutions (ITS) manages all technical standards and maintains a full camera inventory (Section III.D).

UCR Policies and Procedures

A. Operational

1. System Approval and Installation

- a. **Process:** All proposed new installations, changes to, or removal of cameras or systems will be reviewed by UCPD, ITS, and the Camera Governance Group. The Chief of Police, or UCPD designee, is the approving authority on all cameras and their uses in scope of this policy.

The Chief of Police, or UCPD designee, must establish, maintain, and disseminate the review and approval processes to campus stakeholders. The review and approval process shall ensure that proposed changes or installation of new cameras adhere to this policy. The purpose, justification, location, field of view, Privacy impact considerations (see Section III.B - Privacy and Ethical Standards), ownership, Operators, and system capabilities shall be documented by UCPD and ITS. Final design of any installation will be determined through collaborative effort of UCPD, ITS, and requester.

- b. **Emergency Deployment:** UCPD can authorize the immediate installation of cameras in response to urgent operational needs necessary to protect individuals, property, or University operations.

Emergency deployments must be reviewed for continued necessity and compliance with this policy at the earliest reasonable opportunity.

- c. **Standards:** The Chief Information Officer (CIO), in collaboration with the Chief of Police, shall establish standards for device quality and technical integration.

2. Design & Construction Review / Approval

- a. **Adherence to Standards:** Planning, Design & Construction (PD&C) will ensure the latest standards (see Section III.A.1.c - Standards) are used for construction or renovation projects.
- b. **UCPD Design Review:** UCPD must be part of the design review process of any construction or renovation project on University Property that includes camera systems. All proposed cameras will follow System Approval and Installation processes described above.

3. Prohibited Practices

- a. **Non-functional Equipment:** The use of "dummy" or decoy cameras is strictly prohibited.
- b. **Personal Devices:** The use of personal devices to conduct surveillance on University Property is prohibited.
- c. **Unapproved Deployment:** Any installation of a camera without formal approval as defined in this policy is prohibited and subject to removal at the installer's expense. Also see Section III.F.

UCR Policies and Procedures

B. Privacy and Ethical Standards

1. **Privacy:** UCR is committed to upholding the principles articulated in UCR's [Privacy Statement](#). Cameras and Video Data may be used for law enforcement, security purposes as permitted by University policy (including formal investigations conducted under policy), legal compliance, or as otherwise permitted by state and federal law.
2. **Restricted Locations:** Cameras are strictly **prohibited** in locations where community members have a reasonable expectation of privacy.

Restricted locations include, but are not limited to:
 - a. Restrooms, locker rooms, shower facilities, and changing areas.
 - b. Private faculty or staff offices unless specifically approved (See Section III.B.3 - Employee Monitoring).
 - c. Residential spaces (e.g., residential rooms and apartments).
3. **Video Data of Employees:** Using Video Data for timekeeping is strictly prohibited, unless authorized by policy or collective bargaining agreement. Using Video Data for performance issues requires prior approval from UCR Employee and Labor Relations. (Ref UCR HR Policies)
4. **Video Data of Minors:** Use of cameras and Video Data that captures minor children will be in compliance with all campus and applicable state and federal law.

C. Camera Governance Group

1. **Camera Governance Group:** The Provost will establish this administrative body to advise the Chief of Police and to function as described above in Section II.
2. **Request Review:** The Camera Governance Group will review all proposed new installations, changes, or removal of core campus cameras and make a recommendation considering several factors, including but not limited to, privacy, ethical standards, campus safety needs, and available funding.
3. **Camera Maintenance:** UCPD and ITS will work directly with the Camera Governance Group to prioritize camera maintenance needs based on available funding.
4. **Funding Requests:** UCPD and ITS will be responsible for creating annual budget requests for core campus cameras in collaboration with the Camera Governance Group.

D. Inventory and Documentation

1. ITS, in coordination with UCPD, shall maintain a master inventory of all camera systems within the scope of this policy.

Each system must include documentation of:

- Approval authority and date
- System purpose and justification

UCR Policies and Procedures

- Location and field of view
 - Privacy, if applicable, and Ethical considerations
 - Capabilities (video, audio, PTZ, etc.)
 - List of Operators
 - Ownership
2. Camera inventory lists and Operator lists shall be reviewed at least annually by UCPD.
 3. Requests for access to inventory lists will be reviewed by UCPD to determine appropriateness of request.

E. Access & Data Management

1. **Standing Access:** Only designated UCPD and ITS personnel have standing access to Video Data. All other individuals must request authorization as described in this section.
2. **Operator Access:** Access is restricted to Operators who have completed UCPD-led training and have been approved by the Chief of Police and CIO. The Chief Compliance Office may be consulted on access requests as appropriate (See Section III.B - Privacy and Ethical Standards). The Office of Legal Affairs shall be consulted on access requests.
 - a. **Internal Requests:** The Director of Audit & Advisory Services, Locally Designated Official, Civil Rights Officer, Risk Manager, and Chief Human Resources Officer, or their designees, may access upon request for audits, investigations, or assessment of matters including under University or campus policies. Access shall be limited to what is reasonably necessary.
 - b. **Other Requests:** All other requests not covered in subsection III.E.2.a. must be approved by UCPD and/or routed through the Campus Office of Legal Affairs. Requests that are not part of authorized access will be processed under the Public Records Act and/or Information Practices Act, as applicable.
 - c. **Auditability:** All system access must be logged and is subject to periodic audits.
 - d. **Continuous Monitoring:** Is not conducted unless justified by specific operational needs.
3. **Retention and Release**
 - a. **Continuous Retention:** Video Data will be preserved for 14 days.
 - b. **Motion Detected Retention:** Video Data will be preserved for 30 days.
 - c. **Cash Handling Retention:** Video Data will be preserved for 60 days.
 - d. **Extended Retention:** Video Data shall be preserved for a defined period of time when

UCR Policies and Procedures

- i. Required for criminal or administrative investigations;
- ii. Directed by the Chancellor, Campus Office of Legal Affairs or the Chief Compliance Office;
- iii. Necessary to comply with state and federal law.

Preserved Video Data must be destroyed when the extended preservation requirement period ends.

- e. **Release of Data:** UCPD and ITS Security Office may export or release data. All requests for Video Data shall be routed to UCPD for review and release as appropriate.

F. Accountability and Violations

All Operators must formally, and in writing, acknowledge their understanding of, and agreement to comply with, this policy. Non-compliance or unauthorized use (such as exporting data via personal email or screenshots or inappropriate system creation) may result in:

- Disciplinary action or student sanctions under applicable policies and procedures
- Termination of employment
- Civil or criminal liability.

G. Inspection and Maintenance

1. **UCPD Inspection:** All cameras shall be inspected virtually by UCPD monthly to ensure proper operability.
2. **Maintenance Schedules:** UCPD and ITS will be responsible for creating, managing, and updating a preventive maintenance schedule for all cameras, including cleaning, repairs, replacements, and updates.

IV. Responsibilities

The management of camera systems is divided between specialized campus entities to ensure operational integrity and technical compliance.

1. **Chief of Police (Designated Campus Authority):** Authority for all system installations (as well as changes and removals), approvals for Video Data access, and data releases. Ensures compliance with applicable laws, UC Policy, including this policy. Approves deployment, significant changes, and exceptions.
2. **UC Riverside Police Department (UCPD):** Manages administrative use, access control, system monitoring and inspection, and training.
3. **Information Technology Solutions (ITS):** Responsible for setting technical specifications that meet campus standards and maintains sole authority over system infrastructure, system administration, and approved security data forensics. Responsible

UCR Policies and Procedures

for the technical support of the campus-managed camera system(s). Reviews installation and change requests. Maintains master inventory, in conjunction with UCPD.

4. Camera Governance Group: See definition in Section II.

V. Appendices and References

A. Procedures: Procedures or guidelines may be established to support implementation of this policy.

B. References: This policy is established in accordance with the laws, regulatory mandates, and organizational policies linked below.

- [CA Public Records Act](#)
- [UC Electronic Information Security IS-3](#)
- [UC Records Retention Schedule](#)
- [HIPAA](#)
- [UC Statement of Privacy Values](#)
- [UCR Principles of Community](#)
- [UC Unmanned Aircraft System \(Drone\) Policy](#)
- [UCR Campus Filming \(700-15\)](#)
- [California Penal Code Section 632](#)
- [UCPD Departmental Policy Manual](#)

VI. Approval and Revision History

This is the first version of this policy. [Information on approval date to come.]