

**CALIFORNIA INSTITUTE OF TECHNOLOGY  
ADMINISTRATIVE GUIDELINE**

|  |   |
|--|---|
| <b>Subject:</b><br><br><b>Use of Safety and Security Camera Guidelines</b>   | <b>Pages:</b> 5<br><b>Date:</b> September 1, 2023 |
| <b>Approved by:</b> Julia M. McCallin, Associate Vice President for Human Resources and Chief Human Resources Officer (CHRO) |   |

## OVERVIEW

Caltech is committed to promoting the safety and security of the Caltech community. Consistent with these objectives, the use of Video Camera Systems may be approved for safety, security, and other legitimate Institute purposes (“approved purposes”). The use of cameras for approved purposes shall be carried out in a professional, ethical, and legal manner consistent with Caltech policies, programs, and procedures. The installation and use of Video Camera Systems on Caltech premises that do not meet these guidelines or are used for research is prohibited.

### Purpose

These Guidelines address the approval, purchase, installation, use, operation, and maintenance of Continuously Monitored Video Camera and Video Camera Systems (“cameras”) on Institute premises. These Guidelines also address the proper management of any data collected through these devices, which applies to accessing, viewing, storage, retention, and the dissemination of data collected which will be handled in accordance with applicable privacy protections.

The use of cameras to monitor or record data for research purposes (Research Cameras) is not subject to approval under this policy, contact Office of Research Compliance for Research Cameras. Consistent with the Research Camera Guidelines, cameras that record audio, human participants, or animal subjects must be approved by the cognizant research compliance committee.

### Definitions

**Dummy Camera:** A decoy device deliberately designed and positioned to appear that an area is monitored by a Video Camera System when it is not.

**Private Spaces:** Settings where an individual has reasonable expectation of privacy and being free from safety and security cameras. The following are some examples of Private Spaces: residential living quarters, bathrooms, locker rooms, private offices, and designated lactation rooms.

**Research Camera:** A Video Camera System, which can include audio capture as well as video, used exclusively for the purposes of research. Research Cameras can be used to study environmental or mechanical systems, human participants, and animal subjects. Research Cameras can also be used in conjunction with autonomous vehicles for navigation or observation purposes. Research Cameras do not include cameras installed for approved purposes. Contact the Office of Research Compliance for Research Cameras.

**Sensitive Areas:** Settings determined to be high risk and that require special protection. Examples may include data centers, power facilities, facilities with specific security requirements, areas that house hazardous or controlled substances, animal care facilities, areas in which the exchange of currency or other forms of payment occur, and certain laboratory spaces.

**Video Camera System (“cameras”):** The video camera and associated electronics, electrical, software and hardware

systems necessary for installation and use. Any equipment used to capture and/or record video data and/or any visual data (e.g., photos). Cameras may also have the capability to capture audio.

**Video Data:** Visual images, including photos, captured by a camera whether viewed live or previously recorded, that can be replayed, stored, and/or deleted. This does not include data collected by Research Cameras.

### **General Principles**

Cameras for safety and security at Caltech must be purchased, approved, installed, maintained, and accessed according to these Guidelines. Use of cameras for safety and security purposes at Caltech must be limited to applications that do not violate a person's reasonable expectation of privacy as defined by law and Caltech policies. Video Data and associated information obtained from such cameras must be handled with an appropriate level of security and confidentiality to protect against unauthorized access, alteration, or disclosure.

Unauthorized access to, inadequate protection of, and inappropriate use, disclosure, and/or disposal of Video Data and associated information obtained from approved cameras must be immediately reported to the Campus Security.

### **Approval**

Campus Security must pre-approve the use of a camera for safety and security purposes prior to the purchase and installation or use of any device or system. Requests for camera systems are received and vetted by Security through an [online form](#) in consultation with the appropriate Division Operations Officer or Department Head. Any requests for cameras to be installed must be submitted through the Department or Division. Once approved, the installation of a camera must be documented by and coordinated with Campus Security, IMSS and Facilities.

### **Appropriate Use**

Cameras can be one of many effective tools used to support the safety and security of the community. Cameras have been shown to deter violations and crime and, in the event of a reported incidence, can assist in identifying when, where, and how a crime or violation occurred and facilitate authorities in resolving a matter. Video Data captured or recorded by such cameras are subject to controls on viewing Video Data. Video Data and associated information obtained from camera may only be viewed, monitored, reviewed, or otherwise used for the following purposes:

1. To protect persons, buildings, and property;
2. To assist with the investigation of alleged illegal activity or suspected violation of Caltech policy;
3. For facilities maintenance purposes;
4. For maintenance or to verify the camera is operating with full functionality;
5. To monitor Sensitive Areas; or
6. To comply with legal obligations to preserve, release, or otherwise use information.

### **Prohibited Use**

Cameras, including Research Cameras, must not be installed, or used in Private Spaces.

Generally, individuals residing in Caltech housing are not permitted to install exterior or interior cameras (Ring, etc.) Cameras are prohibited inside Caltech Housing premises; baby monitors must be registered with Campus Security utilizing the online form. Exceptions must be registered with Campus Security and in accordance with Student Housing or Faculty Housing. Cameras will be subject to Campus Security verifying the camera is installed and may inspect the angle the camera is recording. If an exception is granted for interior camera installation, employees who are assigned work at the property will be advised through a notification contained in the work order.

Cameras may not be installed in bathrooms, locker rooms, rooms designated for lactation or other activities where a person has a reasonable expectation of privacy, or in residential rooms or apartments in student housing.

Cameras must not record audio without prior written approval from Human Resources. Research Cameras that record audio should be handled in accordance with the Office of Research Compliance.

Dummy Cameras are prohibited.

Hidden cameras, including Research Cameras, are prohibited, unless specifically authorized in advance as part of an investigation and with appropriate prior approval.

Cameras (e.g. phones, laptops, dashcams) personally owned by faculty, staff, or students may not be used for safety and security purposes on Caltech properties.

## **Storage & Security**

Video Data from cameras must be secured and protected to prevent unauthorized access, modification, duplication, and/or destruction.

Suspected unauthorized use of or access or tampering with a camera or Video Data must be reported to Campus Security immediately upon discovery.

For additional information, see Procedures Section E. Access and Data Retention.

## **Roles & Responsibilities**

### Division/Departments –

- Submit a request for approval of cameras to Campus Security.
- Ensure compliance with these Guidelines.

### Campus Security –

- Maintain a list of all Caltech camera's locations covered under this Guideline.
- Receive and review all requests for installation of cameras for Video Safety and Security.
- Review and approve/deny existing and proposed cameras on the Caltech campus.
- Facilitate the purchasing and installation of all cameras.
- Coordinate with IMSS on installation and requirements for cameras using internet capabilities.
- Ensure that any legally required signage is in place prior to use of cameras.
- Coordinate with appropriate departments to secure the Video Data and ensure appropriate access.

### Caltech Facilities –

- Coordinate with Campus Security and IMSS when Cameras are to be installed in new construction and existing buildings as part of construction projects.
- Review and approve placement of proposed Cameras in coordination with Campus Security and Division/Department.
- Coordinate installation of appropriate signage.

## **PROCEDURES**

### **A. Approval**

All Cameras must be registered with the Institute through Campus Security; this applies to all existing systems and any future systems.

An Office/Department must obtain prior approval from the Campus Security before purchasing, installing, or implementing a Camera or implementing a significant change to an existing camera.

A significant change that requires Campus Security approval includes, but is not limited to, the following:

- Changing the area monitored by the camera.
- Changing a Video Camera System from one that is not continuously monitored to one that is a Continuously Monitored Video Camera System.
- Changing the Office/Department responsible for the camera.

- Changing or expanding access to the camera or Video Data.
- Changing to a new camera device or system from the one initially installed.

To obtain approval to install a camera or implement a significant change to an existing camera, an Office/Department must submit the request in writing to the Campus Security Office online form through [access.caltech.edu](https://access.caltech.edu) -> Caltech Help -> Campus Security: <https://help.caltech.edu/helpdesk/WebObjects/Helpdesk.woa>

Every Request should include:

- Location
- Reason for camera
- Department/Division approver

Campus Security will review the camera request. They will consult with other departments on campus, as appropriate. Campus Security will consider the physical security of the location, the existing security programs and operations, the needs to the requestor(s), alternatives to installing a camera, and the camera's compliance with Caltech Policies, including Caltech's prohibition on using equipment that violates the National Defense Authorization Act, Section 889 (NDAA, Section 889).<sup>1</sup> For additional information, visit [Caltech's NDAA Section 889 webpage](#).

Cameras that are installed, or that undergo a significant change, without prior approval from Campus Security are subject to immediate removal.

### **B. Approval of Previously Installed Video Camera Systems**

Within 90 Days of this issuance of these Guidelines, all Divisions/Departments shall submit a written request to Campus Security through [access.caltech.edu](https://access.caltech.edu), Caltech Help, Campus Security [online form](#) for continued use of an existing camera. Continued use of the camera will not be approved unless the camera and its operation and maintenance are in conformity with these Guidelines. Cameras operating outside these parameters will be disabled and removed from the campus network by IMSS with a request to the system owner to remove the camera. If the camera owner cannot be identified the camera will be removed.

### **C. Procurement and Installation of Video Camera System**

The relevant Division/Department is responsible for the funding, operation, and maintenance of any installed camera. After having received approval from Campus Security to proceed, the Division/Department must procure through Campus Security, install, and/or use the camera in accordance with these Guidelines, Caltech policies, including Caltech's prohibition on using equipment that violates NDAA, Section 889. An initial fee for the ongoing network support and storage will be included in the purchase of the camera.

Installation of cameras must be done in accordance with these Guidelines and all applicable Campus policies. All installations must conform to any requirements imposed by Campus Security, IMSS and Facilities.

Campus Security is responsible for developing and maintaining a master inventory of all approved cameras. Camera installations made prior to these Guidelines shall be incorporated into the master inventory.

### **D. Signage**

Signage providing notice of the presence of cameras shall be posted in accordance with any requirements, instructions, and specifications stipulated by Campus Security upon their approval of a camera installation.

Cameras installed without proper signage are subject to immediate removal.

---

<sup>1</sup> Caltech must comply with federal laws and regulations regarding the Prohibition on Certain Telecommunications and Video Safety and Security Equipment (Reference: The National Defense Authorization Act, Section 889). These regulations impact both the administrative and research community regarding the purchase and use of specific telecommunications and video safety and security equipment. As a federal awardee, Caltech is subject to these prohibitions. Therefore, if you purchase or use goods or services (Video Camera Systems) on behalf of Caltech, you must not purchase or use any equipment, system, service, or component thereof produced or provided by prohibited companies, their subsidiaries, or their affiliates. Please consult with the Director of Procurement Services for additional information.

## **E. Access & Data Retention**

1. Recorded Video Data and associated information, subject to these Guidelines, will be stored in a secure location with access by authorized personnel only.
2. Access to Video Data, subject to these Guidelines, must be approved by Campus Security or other organizations as appropriate.
3. Video Data will be stored consistent with Caltech's [Record Retention Schedule](#) storage of video camera footage and will generally not exceed 30 days, unless a longer retention period is warranted.
4. Requests to access Video Data are managed and controlled by Campus Security, who will consult with other organizations as appropriate.