Columbia University
Department of Public Safety

Effective Date: September 2020

Closed-Circuit Television (CCTV)
Monitoring and Recording For Safety and Security Purposes

1. Purpose

This policy concerns the installation and use of CCTV to monitor and record areas for the purposes of safety and security.

2. Scope

This policy is applicable to all students, faculty, staff, vendors, and other visitors on Columbia University owned, leased, and controlled property and including surrounding public areas (*e.g.*, sidewalks outside a University building).

This policy does not address the use of recording equipment for educational or research purposes by approved University personnel. Examples include recording of research experiments or projects, lectures, interviews, concerts, athletic events, plays, or other public performances. Such recording may be subject to other policies governing research with human subjects and academic, privacy and event-specific policies, as well as applicable federal, state and local laws. This policy is not intended to create any contractual rights.

3. General Principles

Columbia University Department of Public Safety (DPS) is committed to enhancing the safety of the campus community by integrating best practices of campus safety and security with enhanced technology. A critical component of a comprehensive campus security and crime prevention program is the use of CCTV.

Video monitoring and recording for safety and security purposes will be conducted in a professional, ethical, and legal manner.

Video monitoring and recording for safety and security purposes will be conducted in a manner that respects the reasonable expectation of privacy among members of the community.

All video monitoring and recording will be conducted in a manner consistent with all existing University policies, including the *EOAA Policies & Procedures* (the "Non-Discrimination Policies") and other relevant policies.

Monitoring based on the characteristics and classifications contained in the Non-Discrimination Policies (*e.g.*, race, color, religion, sex, age, national origin, disability, pregnancy, sexual orientation, marital status, familial status, status as a victim of domestic violence, alienage or citizenship status, creed, genetic predisposition or carrier status, unemployment status, or any other protected status or characteristic as established by law) is strictly prohibited.

Violations of this policy may result in disciplinary action consistent with the policies governing employees of the University.

4. Location

Cameras used for CCTV may be installed at the direction of DPS's Vice President for Public Safety or designee in any location except for the following:

- Dormitory rooms, apartments, and residential units for students, faculty, and staff;
- Restrooms and bathing facilities;
- Locker rooms and other changing facilities; and
- Offices of individuals (except where requested by occupant).

The prohibitions in the foregoing list refer to camera installations that would allow the surveillance of the interior of the designated locations. For example, the policy does not allow the installation of cameras in a dorm room or outside of but looking in the window of a dorm room. On the other hand, the University may have valid reasons, under the terms of this policy, to have cameras looking, for example, at the exteriors of dorms or at the entrances to classrooms and offices.

Signage or other forms of notice, specific or general, stating the presence of cameras is permitted but not required. Cameras will be installed in locations that are open and conspicuous and will not be activated or configured to record audio.

In situations involving threats to the safety of the campus, to the life, health or safety of any person, or of theft or destruction of property and upon consultation with the Office of the General Counsel (OGC), temporary exceptions may be made to the prohibitions in the foregoing list.

5. Installation, Monitoring and Recording

CCTV may only be used to monitor and record for legitimate safety and security purposes including, but not limited to, the following:

- *Criminal investigation*
  Robbery, assault, theft surveillance, etc.
- *Video monitoring of public areas*

Transit stops, parking lots, public streets near campus, bike racks, University artwork and sculptures, etc.

- *Protection of buildings and property*
  Building perimeters, cashier locations, and entrance and exits of: lobbies and corridors, receiving docks, special storage areas, laboratories, etc.
- *Verification of security alarms*
  Intrusion alarms, exit door controls, etc.
- *Monitoring of access control systems*
  Restricted access transactions at entrances to buildings and other areas
- *Protection in highly sensitive laboratory environments*
  Laboratories containing materials or hosting activities that are highly sensitive or dangerous and thereby raise health, safety and/or national security concerns
- *Compliance with government requirements*
  Pursuant to laws and other government requirements pertaining to public safety and security

Data obtained through CCTV may be accessed and/or used for safety and security purposes and in limited other situations, including:

- To help prevent or deal with situations presenting threats to the safety of the campus or to the life, health, or safety of any person or the theft or destruction of property;
- The investigation or prevention of crime or violation of University policy;
- In connection with threatened or pending litigation by or against the University and to respond to, or in connection with, lawful demands for information in law enforcement investigations, other government investigations, and legal processes; and
- To document or monitor the progress of construction projects.

6. Maintenance of CCTV Data

Data from CCTV (*e.g.*, surveillance footage) is maintained consistent with the storage capacity of the recording device (*e.g.*, many storage devices are automatically overwritten after 30 days, although this varies). CCTV data will be otherwise preserved for longer periods pursuant to a lawful order, in connection with litigation or potential litigation, or as part of a University or governmental investigation or an agency or court proceeding (criminal or civil).

CCTV may only be accessed and/or used by authorized DPS personnel. If authorized DPS personnel identify a legitimate institutional need, it may be shared with other authorized University personnel on a need-to-know basis only.

CCTV data will be treated sensitively and will not be shared outside of the University except (a) to its authorized agents (*e.g.*, attorneys or insurance providers) on a need-to-know basis, (b) subject to a lawfully issued subpoena or court order, or (c) as needed to law enforcement or other public officials in the case of an emergency situation involving threats to the safety of the campus, to the life health or safety of any person, or of theft or destruction of property. Notwithstanding the foregoing, distribution of CCTV data through Clery Crime Alerts and equivalent warnings are permitted use.

7. Responsibilities

a. Columbia University Department of Public Safety (DPS)
    i. DPS is the sole department authorized to have full administrative rights to CCTV data and other technology. All CCTV data will be stored in a secure location with access by authorized personnel only.
    ii. All DPS personnel with access to CCTV data will receive a copy of this policy and provide written acknowledgment that they have read and understood its contents.
    iii. The Vice President for Public Safety or designee will determine which DPS personnel are authorized to access CCTV data.
    iv. DPS's Executive Director of Investigations or designee may authorize other non-DPS personnel to access CCTV data on a specific and limited need-to-know basis for any authorized purpose.
    v. The Executive Director of Investigations will maintain a log of non-DPS personnel given access to CCTV data other than Office of the General Counsel (OGC) personnel responding to subpoenas, court orders, or threatened or pending litigation. The log will include personnel names and titles, reason(s) the CCTV data was sought, time/date/location provided, who authorized the access, any further use or distribution of data, and affirmation that the non-DPS personnel understands their obligation to perform duties in accordance with this policy.
    vi. Authorized DPS personnel will be trained in the technical and ethical parameters of appropriate CCTV access and use.
    vii. DPS's Executive Director of Technology will monitor developments in security industry practices to ensure that DPS's practices are consistent with best practices.
    viii. DPS will consult with OGC upon receipt of a subpoena or court order for CCTV data.

b. Other
    i. Individual schools, departments, programs, campus organizations, or any affiliates of the University wishing to change, install new, or expand CCTV camera coverage may submit a request for consideration to DPS's

Executive Director of Technology or designee. As applicable, the request should include (1) a description of the safety, security, or other issue warranting the change or installation of the camera(s); (2) proposed location of the camera(s) to be installed; and (3) funding source(s) for initial installation of the equipment and ongoing annual maintenance. The Executive Director of Technology or designee is responsible for taking project management lead for all aspects of CCTV projects, including schedules, plan design and execution, and the management of funding sources for new installations.

ii. The Executive Director of Technology is also responsible for working with Columbia University Information Technology Department (CUIT) to ensure network quality of service and all technologies related to network connectivity, bandwidth and security planning, including applying best practices to meet the demands and expectations of the system, physical security, and applying security to ensure the CCTV system is best protected from unnecessary interruption and/or intrusion.

c. CCTV Governance Panel

i. There shall be a CCTV Governance Panel which will consist of six individuals representing the following offices: DPS, OGC, Facilities, Human Resources, the Provost's Office, and Community Affairs.

ii. The Panel will meet at least once annually to receive reports from DPS on CCTV practices and to ensure appropriate implementation of this policy. The reports will include information as requested about CCTV usage, including new or changed camera locations; access logs; community requests and all complaints or concerns; policy exception summaries; and other updates and developments.

iii. The CCTV Governance Panel will review this policy periodically and recommend revisions if needed.