POLICY ON INSTALLATION AND USE OF VIDEO CAMERAS

Effective May 25, 2016

A. Scope of Policy

This policy concerns the installation and use of video cameras anywhere on the Harvard campus for safety, security and facilities management purposes (meaning the use of video cameras to support safe and efficient facilities operations). This policy applies to all Schools and units of the University.

This policy does not affect other Harvard policies on use of video cameras, such as policies on videotaping conferences or lectures, in the classroom, for research purposes, or for public dissemination.

B. General Statement

Use of video cameras has become ubiquitous in our society. This includes use on the Harvard campus and in our facilities, where video cameras have been installed to serve various institutional purposes. In installing and using such cameras, the University needs to be both orderly and transparent.

This policy sets out guidelines and requirements for the installation and use of video cameras for safety, security and facilities management purposes. This policy is intended to establish internal standards and procedures governing such use of video cameras on campus; it is not meant to create rights in any individual to seek legal redress for action inconsistent with the policy.

C. Authorization

Each School or other Harvard unit shall designate one or more persons who will have the authority to review and approve all requests

(a) for installation of video cameras in or on the facilities, property or vehicles (including drones) of that School or unit for safety, security and facilities management purposes, subject to the guidelines in part D; and

(b) for access to data from any video cameras installed by that School or unit, subject to the guidelines in part F.

The Schools and units may decide that different people may perform these two functions.

D. Guidelines for Installation

D1. Video cameras to be used for safety, security or facilities management purposes may be installed in any location except for the following;

(a) dormitory rooms;

(b) the living quarters of other residential facilities;

(c) restrooms and bathing facilities;

(d) locker rooms and other changing facilities;

(e) classrooms; and

(f) offices of individuals.

These restrictions do not limit video camera use pursuant to other University or School policies, or with respect to important and sensitive institutional functions that are customarily monitored, such as cash management or lab safety.

The prohibitions in the foregoing list refer to camera installations that would allow the surveillance of the interior of the designated locations. For example, it is not appropriate to install cameras in a dorm room, or outside of but looking in the window of a dorm room. On the other hand, the School or unit 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.

The foregoing list establishes mandatory restrictions on the placement of cameras, but is not intended to be exhaustive. A School or unit may impose further location restrictions where it is believed that the presence of cameras would be inconsistent with community values, the preservation of an environment that encourages free academic and intellectual inquiry, or other important values.

D2. In exigent 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, temporary exceptions may be made to the restrictions in D1, or to similar additional restrictions adopted by a School or other unit, provided that the Office of the General Counsel (OGC) shall be consulted if time allows.

D3. Signage or other forms of notice, specific or general, stating the presence of video cameras is permitted but not required. Camouflage or other deliberate concealment of cameras is not permitted unless specifically requested by the Harvard University Police Department (HUPD) after consultation with OGC.

D4. Unless requested by HUPD for safety, security or law enforcement reasons in compliance with Massachusetts law, video cameras installed for safety, security and facilities management purposes shall not be configured or activated to record audio.

E. System Operation

E1. Each School or other Harvard unit shall designate one or more persons who will have day-to-day responsibility for acquisition, installation, and operation of video cameras for safety, security and facilities management purposes.

E2. Video cameras and supporting systems should comply with any University-wide video technology standards as established by HUIT so that all systems will be compatible and will be accessible by HUPD via the University network for safety, security or law enforcement reasons. Where appropriate, such equipment should be acquired from vendors designated by the Office of Strategic Procurement.

E3. Technology for storage of data and procedures for data transfer shall comply with data security standards established by HUIT.

E4. Each School or unit should establish guidelines for (i) how long cameras should be in place, (ii) which cameras should be operated intermittently and which continuously, and (iii) which cameras should provide live feeds for real time monitoring.

E5. Each School or unit should establish guidelines for how long data will be retained, provided that all data should be retained for at least one month.

F. Guidelines for Access to Data

F1. Video camera data may be accessed for the following purposes:

(a) the investigation or prevention of crime;

(b) 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;

(c) 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;

(d) in connection with investigations of misconduct by members of the University community, if the investigation would advance a legitimate institutional purpose and there is a sufficient need for access to the data;

(e) in support of and to review facilities operations;

(f) to document or monitor the progress of construction projects;

(g) incidentally in connection with maintenance, management and inspection of video camera and related technology to ensure proper operation, to protect against threats

such as intrusions and other attacks, malware and viruses, and to protect the integrity and security of the data; and

(h) for other comparable reasons that advance a legitimate institutional purpose.

- Except as provided above, video camera data may not be accessed in connection with administration of ordinary personnel matters.

F2. Each School and unit should establish a procedure for implementing access to video camera data in order to provide that the data will be accessed for purposes, and by personnel, as permitted under this policy.

F3. All access requests must state the reason the data is sought and reasonably specify the relevant date, time and location. In all cases, access must comply with applicable legal requirements. Any authorization of access should apply only to the particular situation.

F4. Access to the data, whether recorded or live, should be limited to those personnel with a reasonable need for such access in the particular case.

F5. Schools and units may from to time receive requests for video camera data from outside of Harvard. Recorded data may be provided to a non-Harvard party if the purpose of the request is not contrary to provisions of this policy or the School or unit policy. To be approved, such a request must also comply with paragraph F3. However, the non-Harvard party may not participate in the search for the requested video data (unless required by law) and shall receive only a copy of the particular video segment requested.

F6. In emergency situations, HUPD and other responders may access video camera data without prior authorization. In such cases, they should notify the School or unit and the OGC as soon as practical.

F7. In each case in which video camera data is accessed, the School or unit, and HUPD if it is involved, shall keep appropriately detailed records of the access purposes, the data searched, the relevant data found, who authorized the access, and any further use or distribution of data.

F8. It is not necessary to give general notice, or notice to specific identified individuals, of searches of video camera data (unless required by law).