# Security Camera Policy

*(for discussion only)*

Committee on Information Technology Policy (CITP)
December 19, 2022

*with thanks to Raghu Cowlagi (AE), former CITP Chair, for work on this in AY21-22*

# Background

- Information Security, Risk, and Compliance (ISRC) Committee
  - Now disbanded committee, internal to IT, which created and enacted several policies without CITP's involvement, including Security Camera Policy

- CITP began reviewing Security Camera Policy in Spring 2021, and continued review in AY21-22, with major concerns:
  - Definitions of public/private areas
  - Notification to the community about cameras
  - Ambiguity regarding real-time monitoring
  - Ambiguity about nature of, access to, and retention of data
  - Concern about impact of surveillance on community wellbeing and privacy

# Policy Goals

- Establish internal standards and procedures governing use of security cameras and data collected from them
- Clarify community understanding of security camera presence on campus
- Protect academic freedom and freedom of expression, and minimize negative consequences of surveillance on individuals' freedom, security, and privacy

# Definition of Cameras

- Video camera and supporting infrastructure that is used “specifically and solely for security purposes”

- Only record video, not audio, with two named exceptions:
  - WPI Police Interview Room
  - Mailroom doorbell camera

- The following cameras are *not* security cameras:
  - Classroom lecture capture (see: *Learning Management System & Video Lecture Support Policy*)
  - Video conferencing cameras
  - Video recording of athletic events for post-game review
  - Video recording of human/animal subjects for research
  - Cameras to ensure safe laboratory practices in research labs
  - Body-worn or otherwise portable cameras used during law enforcement operations

# Definitions of Space

Cameras are only allowed in “public areas”, and explicitly not allowed in “academic areas” or “private areas”.

***“Public Areas”*** *refers to areas available for use by the public, including, but not limited to, campus grounds, parking areas, building exteriors, loading docks, staircases, areas of ingress and egress, lobbies, theaters when not used as classroom space, library entrance and socialization space, dining halls, gymnasiums, recreation areas, and retail establishments.*

***“Private Areas”*** *refers to areas in which a person has a reasonable expectation of privacy, including, but not limited to offices of individuals, non-common areas of residence halls, residence hall corridors, bathrooms, shower areas, locker and changing rooms and other areas where a reasonable person might engage in personal activities such as changing clothes. Additionally, areas designed for the personal comfort of WPI employees or the safeguarding of their possessions, such as lounges and locker rooms, and areas dedicated to medical, physical, or mental therapy or treatment shall be considered private areas for the purpose of this policy.*

# Definitions of Space

Cameras are only allowed in “public areas”, and explicitly not allowed in “academic areas” or “private areas”.

***“Academic Areas”*** *refers to areas such as classrooms, lecture halls, study rooms, labs, library study and research areas, or conference rooms that are used specifically for academic purposes. These are areas of public use where privacy is not expected for personal activity (e.g., changing clothes), but, in the interests of academic freedom and freedom of expression, nor is surveillance expected.*

To CITP’s knowledge, this is the first policy at WPI to explicitly designate space as “academic” in nature.

# Realtime Monitoring

- Realtime monitoring expressly forbidden, except in two special circumstances:
  - Compliance with law enforcement orders (no notification to community)
  - Special events, such as commencement (required notification to community)

# Privacy Protections

- Explicitly disallows placebo cameras (if you see a camera, it’s real and it’s recording)
- No use of automated facial recognition by WPI at any time.
- Disciplinary action for anyone found to be video monitoring an individual without probable cause and/or search warrant.
- Security camera recordings may only be used for campus safety purposes, and explicitly may not be used to monitor employee performance.

# Oversight and Compliance

- Recorded footage is only accessible to WPI Police, direct review of video camera footage must be authorized by Chief of Police. IT personnel only have access during installation and maintenance.

- How recording footage is stored is subject to *Records Retention and Destruction Policy* (ISRC Policy, not approved by CITP, under revision/review as of AY21-22)

- Chief of Police must approve any requests for release of recorded material.

- Separation of responsibilities:
  - Chief of Police: maintain records related to use of cameras and recordings
  - IT Infrastructure & Operations: maintain records related to camera and system configuration

- Chief of Police and IT Infrastructure & Operations collaborate to review deployment and utilization of cameras, on no set timescale (“whenever and as frequently as they deem necessary”)

# Questions / Feedback

**AY22-23 Committee on IT Policy**
Gillian Smith (Chair, COG Appointee)
Brigitte Servatius (CAP Appointee)
Xiaozhong Liu (CTAF Appointee)
Rodica Neamtu (Provost's Appointee)
Sia Najafi (*ex officio*, Interim CIO)