WAKE FOREST
UNIVERSITY

Video Surveillance Policy
February 2012

Purpose

Wake Forest University aims to provide a secure environment for members of its community and to protect personal safety and property, assisted by video surveillance systems technology. This policy is intended to regulate the use of video on campus for surveillance purposes, including both monitoring and recording, in order to enhance the campus quality of life and to respect the privacy rights of faculty, staff, students and visitors.

Scope

This policy applies to all WFU employees, students and organizations in their use of cameras for video surveillance purposes.

This policy does not apply to uses of video for non-surveillance purposes. Examples of non-surveillance video are recordings that are made for instructional purposes, for capturing public events and performances, for convenience such as weather or construction site viewing, or for conferencing. Uses of video approved by the University's Institutional Review Board for clinical research are also exempt from this policy. This policy does not address surveillance deployed by University Police, with or without notification, in support of a specific investigation or law enforcement purposes, except as set forth in section VI; University Police are authorized to utilize existing surveillance output of any type for investigative purposes if circumstances arise that warrant it. In addition, this policy does not prohibit the University's Legal and Compliance Departments, either directly or through an agent, from conducting or approving the conduct of an investigation that may include use of video surveillance systems.

Oversight and Administration

The Deacon OneCard Manager and the Wake Forest University Chief of Police shall oversee compliance with this Policy and shall have oversight over all University video surveillance systems covered by this Policy.

The Deacon OneCard office shall be responsible for maintaining overall administration of all University video surveillance systems and equipment subject to this Policy, including but not limited to:

- Approval of all equipment and system software;
- Approval of all installation and service;
- Approval of all camera administrators for primary and secondary purposes;
- Granting administrative and usage permissions;
- Establishment of proper and ethical usage practices;
- Removal of or restrictions on usage as necessary for compliance with this Policy.

All video surveillance systems covered by this Policy may be monitored by University Police and the Deacon OneCard office at any time. In order to properly monitor public areas in accordance with this policy, the Deacon OneCard office and University Police shall have primary control of remotely operated PTZ (Pan Tilt Zoom) cameras.

University Police may access video recordings for investigative purposes. All recorded video shall be maintained within the security access system for a period of 90 days in compliance with the Payment Card Industry Data Security Standard (PCIDSS) as adopted by WFU Information Systems and shall be administered by the Deacon OneCard office.

Policies and Procedures

I. Requirements

Any University department, program, or campus organization that utilizes video surveillance systems must designate an assigned administrator (who must be approved by the Deacon OneCard office) to be responsible for ensuring use of the surveillance system adheres to the requirements of this Video Surveillance Policy.

The assigned and approved administrator will have authority to view live and recorded video captured by the designated camera/surveillance system. The administrator shall not utilize the system in a manner that infringes on the reasonable expectation of privacy of any student, faculty, staff or guest of the University. Video surveillance systems shall be utilized to monitor areas with public access only. Public area is defined as any portion of any Wake Forest University building or facility that is accessible to the general public. Examples of locations where surveillance systems are generally prohibited include bathrooms, gym locker/changing areas and private offices (unless consent by the office user is given). Examples of locations where cameras are generally acceptable include public areas, hallways, entrances and exits of academic, administrative, residential and service buildings; parking lots; gymnasiums; cafeterias; supply rooms; and classrooms.

Views of residences must not be greater than what is afforded by unaided, human vision. Viewing through the windows of private rooms is prohibited. Approval may be granted to specific individuals for temporary use and installation of a video surveillance system in residential hallways and lounges, but only where there is a reasonable belief that there is an imminent security risk or an active investigation.

Utilization of video surveillance systems shall be conducted in a manner consistent with all existing University policies. Operation of video equipment and systems shall be conducted in a professional, legal and ethical manner. Video surveillance of individuals shall not discriminate on the bases of race, gender, sexual orientation, national origin, disability, or age.

The University does not condone use of video surveillance systems as a tool for routine performance management of University employees or the use of personal “webcam” technology for surveillance purposes.

II. Responsibilities of the Deacon OneCard office

Deacon OneCard office is responsible for disseminating this policy on campus, for advising departments on appropriate applications of surveillance technologies, and for assisting departments in preparing proposals for the funding and installation of surveillance equipment.

Deacon OneCard office shall review proposals and recommendations for camera installations and specific camera locations to ensure that the implementation and use of all surveillance cameras conform to this policy.

The Deacon OneCard Manager shall, in consultation with the Chief of University Police or his/her designee, determine the appropriateness of any surveillance camera system installation, weighing the concerns of the person or persons making the requests and the safety and security of the entire community.

The Deacon OneCard Manager shall review complaints regarding camera locations and determine whether the requirements of this Policy are being followed. Appeals of a decision by the Deacon OneCard Manager shall be reviewed by the Dean of Residence Life and Housing which shall make final disposition. This may require consultation with University Policy and Legal.

The Deacon OneCard Manager shall review all requests to release recordings obtained through University owned or leased camera systems and shall consult with the Chief of University Police and the University Legal Department about such requests. No video recording shall be released without authorization from the Deacon OneCard office Manager, after consultation with the Chief of University Police and the University Legal Department.

The Deacon OneCard Manager shall develop an appropriate mechanism for auditing the database of the system on an annual basis, at the very minimum to ensure all records reflect active users of the system.

III. Installation and Maintenance

Any University department, program, or campus organization wishing to install any type of video surveillance system shall consult with the Deacon OneCard office and submit a Security Device Form signed by their Vice President or Dean and Director or Department Chair. The written request shall describe the proposed location of camera devices, the need for the proposed installation and the intended use, and provide the name of the proposed administrator for the individual camera system. The Deacon OneCard Manager shall review all proposals, and after consultation with the Chief of University Police or his/her designee, approve or deny the request. Cameras and the system will be maintained by Deacon OneCard personnel in consultation with Information Systems to ensure compliance with University physical security standards.

IV. Training

University personnel authorized to utilize University owned or leased video and recording surveillance systems shall be appropriately trained by the Deacon OneCard staff in the responsible operation of the system and the technical and ethical parameters of appropriate camera use. Administrators of the individual camera system shall receive a copy of this policy and provide written acknowledgement that they have read and understood its contents and agree to abide by the terms of this policy.

V. Operation

The primary function of video surveillance systems shall be to enhance the safety and security of the University through the monitoring of public areas of access and transit to include both vehicle and pedestrian areas. This policy does not imply or guarantee that video systems will be monitored in real time.

If a surveillance camera is installed where identification of individuals is possible, appropriate signage shall be installed in the area indicating the presence of the camera(s), except at emergency or investigative locations. The sign should state, “This area is subject to video surveillance and may or may not be monitored.”

Any secondary function of video surveillance systems shall be with the permission of the Deacon OneCard Manager and shall be monitored by University Police to ensure full compliance with this policy. Examples of secondary functions include the overall use of video surveillance systems by the University in order to broadcast by means of the World Wide Web (e.g., on the Official Wake Forest University Website), television, brochures, etc.

Any unauthorized use or rebroadcast of video systems or recordings is strictly prohibited. Any violation of this policy may result in revocation of usage permissions, disciplinary action up to and including termination of employment and reporting to the proper authority.

VI. Temporary Surveillance Camera Use

The University Police Department, at the discretion of the Chief of Police or his/her designee, has the authority to use temporary surveillance system cameras for law enforcement purposes. The University Police Department will work with the Manager of the Deacon OneCard office to determine location set-up and efficient monitoring of the temporary surveillance system cameras within the Lenel system.

Forms

Security Device Form

Drafted October 2011

Approved February 2012