# Monitoring Policy

**Purpose and Scope**

- The purpose of this policy is to describe and set limits on permissible monitoring of system activity and computers on the Wofford College campus.
- This policy applies to all Wofford College Information Technology (IT) staff members.

**Policy**

As stated in the College's *Policy on the Responsible and Ethical Use of Wofford College Technology Resources*, Wofford respects the privacy of all electronic communications and files. We will take reasonable precautions to protect information stored in or on, or transmitted by, our system. We do reserve the right to protect the integrity of our technology resources. In particular we claim the right to monitor system activity and, in the case of possible harassment or other violations of College policy and with proper authorization, to examine college computers associated with reported incidents. In all cases, IT staff will follow the principle of least perusal of contents and least action necessary to resolve a situation.

The privacy of user files and network activity is not absolute. IT staff routinely keeps logs of user access to the network and network devices. They also may find it necessary to scan user files or monitor network traffic for security compromises, or for other administrative purposes. This will be done with as much respect as possible for user privacy, and where possible will be done with automated tools which report only essential information to the human administrators.

- Our campus network system, including its computers, is for the use of authorized users only. Individuals using it without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.
- In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.
- Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

The following are specific examples of limits on IT and administrative monitoring:

- **Electronic Mail**: Administrative access to Wofford College email accounts may be used only for official Wofford investigations, law enforcement inquiries, or issues where life and/or property are in jeopardy. All other forms of access to and control of Wofford email accounts is controlled by accountholders, who are responsible for taking appropriate steps to manage their accounts.
- **Banner**: In order to ensure the security of Banner accounts and passwords, IT will periodically record the users who are logged on and the machine they are using. IT will audit an individual's Banner activity only if approved by their supervisor.

- **Desktop/Laptop Computers and Network Storage**: IT furnishes all faculty and staff with a desktop or laptop computer as well as storage space on the campus network.
    - The computers will be jointly managed by IT and the user, as described in the *Computer Management Policy*
    - Although it is permissible to store personal files on these computers and on network storage, anything stored there, with the exception of electronic mail, will be assumed not to be private.
    - When faculty or staff members retire, they should remove all personal files from their computer and network storage before leaving the college.
        - Following retirement, their supervisor and IT staff will be given access to their computer and network storage.
        - Eventually, all stored files, including electronic mail, will be erased.
    - In the event that faculty or staff members are terminated, they will be given the opportunity to retrieve and/or delete personal files from their computer or network storage
        - Both an IT staff member and a member of their former department must be present when they are retrieving personal files.
- **Remote Desktop Monitoring**: IT will remotely monitor an individual's desktop computer activity only under the following circumstances:
    - If the individual gives us his or her explicit consent, in which case a Help Desk ticket will be made on the incident; or
    - If approved by the individual's supervisor and the Vice President of Technology
- **Network Monitoring**: IT will monitor network activity to the extent required to ensure the integrity of the campus network.
- **Telephone Monitoring**: Conversations via telephone lines will not be monitored at any time without a court order. Only law enforcement agencies may enforce a court-ordered telephone line tap. No Wofford College employee may record telephone conversations without the expressed consent of both parties involved. The Telephony Systems Administrator does record call originations and destinations for the purposes of billing, fraud detection, harassment investigation, E-911 regulation compliance and system enhancement.

**Enforcement**

- Continued access to monitoring tools depends on an IT staff member's compliance with the policies outlined herein.
- Failure to abide by these policies could result in access to these tools being discontinued and the possibility of additional disciplinary action.

**Responsibility**

- The responsibility for enforcing this policy lies with the Vice President of Technology, 597-4294.