



Computer User's Guide

to the Electronic Campus



Privacy & Technology	1
Electronic Communications	1
Communications Records	1
Monitoring Communications	2
Report Privacy Violations	2

Northwest and *Information Systems* is dedicated to preserving privacy with regard to the use of technology. However, electronic activities may be subject to the *Freedom of Information Act* and legal investigation requests placed through proper channels when alleged violations are suspected.

Electronic Communications

Under *US Legal Code Title 18*, section **2511** interception and disclosure of wire, oral or electronic communication are prohibited.

Part (1): Except as otherwise specifically provided in this chapter any person who - (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication is in violation of chapter **2511** or the *US Legal Code*.

Also under *US Legal Code Title 18*, section **2511** part (2): "It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider or wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks."

For the full text of section **2511** see:

http://www.law.cornell.edu/uscode/18/uscode_sec_18_00002511----000-.html

Under this chapter of *US Legal Code*, Northwest as a provider of electronic communication service has the legal authority to monitor communications sent across its networks or stored on computer facilities or related electronic equipment for the electronic storage of such communications.

Employees of Northwest's *Information Systems* department can perform this monitoring in the performance of duties related to their employment. These duties can include, but are not limited to administration, troubleshooting, maintenance or repair of network infrastructure, servers, storage device and university owned computers located in residence halls, offices and labs, as well as those issued to individuals. Communication to and from privately owned computers connected to the University network are not excluded from monitoring.

Disclosure of any communications intercepted during performance of the employee's job is prohibited except in situations permitted by federal, state or local laws.

Communications Records



While Northwest does not typically monitor usage of the Northwest network, Northwest does keep a record of all log-on attempts, printing jobs/charges and web pages served from Northwest servers. The information is used by the university for billing and statistical purposes.



Monitoring Communications

The *Information Systems* department does not routinely monitor individual usage of campus computing resources. However, users should also be aware that their use of Northwest's computing resources is not completely private.

The normal operation and maintenance of campus computing resources requires the backup and caching of data and communications. Thus, the logging of activity, the monitoring of general usage patterns, and other such activities are necessary for the rendition of service and network stability.

Information Systems may also specifically monitor the activity and accounts of individual users of Northwest's computing resources (computer stations and network infrastructure), including individual log in session and communications, without notice when:

- (a) the user has voluntarily made them accessible to the public, as by posting to *Usenet* or a web page;
- (b) it reasonably appears necessary to do so to protect the integrity, security or functionality of University or other computing resources or to protect the University from liability;
- (c) there is reasonable cause to believe that the user has violated or is violating this policy;
- (d) an account appears to be engaged in unusual or unusually excessive activity as indicated by the monitoring of general activity and usage patterns;
- (e) or it is otherwise required or permitted by law.

Any such individual monitoring, other than the specific in "(a)", required by law or necessary to respond to perceived emergency situations, must be authorized in advance by the *Vice President of Information Systems* or the *Vice President of Information Systems designee*.

The *Information Systems* department, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications to appropriate campus personnel or law enforcement agencies and may use those results in appropriate campus disciplinary proceedings.

Communications made by means of campus computing resources are also generally subject to *Missouri's Public Records Statute* to the same extent as they would be if made on paper.

Report Privacy Violations

Any violations of this privacy policy should be immediately reported to the appropriate Northwest official.

Disciplinary action of any violations will be handled in accordance with Northwest policies and regulations or local, state and federal law.

Violations of privacy should be reported to the *Vice President of Information Systems*, the *Vice President of Information Systems* designee or *Campus Safety*.

If you are the victim of a privacy violation or suspect a privacy violation, contact *Campus Safety* at 660-562-1254 or contact the *Client Computing—Information Systems* Help Desk at 660-562-1634.

