LINCOLN UNIVERSITY

Policy:	**Computer and Network Usage by Employees**
Policy Number:	**HRM-110**
Effective Date:	**July 1, 2009**
Revisions:	**Replaces, as they relate specifically to employees, IT Policies 517 – Internet Usage; 518 – Internet Monitoring; 519 – Internet Privacy Policy; and 804 – Use of Portable Computers, August 2011**
Next Review Date:	**August 2013**
Review Officer(s):	**Chief Human Resources Officer and Chief Information Technology Officer**
Status:	**Approved by President and Active**

1. Purpose of Policy

The purpose of the Lincoln University Computer and Network Usage Policy for Employees is to help provide guidance and codify in one place the policies and guidelines with respect to the appropriate use by employees of Lincoln University's computer system and network and related information technology resources. It is further intended to help ensure that the information technology infrastructure that supports the fundamental missions of the University is properly safeguarded and appropriately used by employees in discharging their duties.

2. Applicability

2.1 This Policy is applicable to all employees of Lincoln University who are granted the use by the University of, or who otherwise use (even without proper authorization), the University's computers and related information technology resources, including the University's computer equipment, systems, and networks, as well as the information, data, communications and files created, sent, received or stored therein. It also applies to employee use of all related computer system resources, whether individually controlled or shared, stand-alone or networked, including all networking devices, personal digital assistants (PDA devices), wireless computer devices, personal and portable computers, tablets, workstations, mainframes, minicomputers, and any associated peripherals, hardware, software, and programs, that are owned, leased, or under the control of the University or form part of the University's computer network, system or computer equipment. All of the computer systems and technology and data and electronic communications covered by this Policy are hereinafter referred collectively to as "University Technology."

2.2 This policy applies specifically to employees of the University. Separate Information Technology Department ("IT") policies of the University apply to students and other permitted non-employee users of University Technology. Separate policies also apply to use by employees and others of University telephones, walkie-talkies and other communication devices that are not part of the University computer system.

3. General Principles

3.1 Certain University employees, as part of their employment, may be provided by the University with access to, or the use of, University Technology, including in certain circumstances access to computers, hardware, software, the use of the University's network and email systems, and access to the internet. Such University provided access to University Technology is to be used by the employee in support of the proper performance of his or her duties on behalf of the University.

3.2 The University is committed to reasonably protecting the privacy of all individuals using University Technology, including the University's students, employees, and others who are permitted access to or communicating through the University Technology. Employees should understand, however, that all employee communications, data, and files stored on or traversing the University's network and system, or stored on the University's servers and hardware, are considered the property and the business records of the University. As is explained in more detail below in Section 9 of this Policy, the University reserves the right, to the extent permitted by law, to monitor and review employee computer files, data, email and other electronic communications, internet use, including sites visited, and other uses of University Technology by employees, as well as the right to inspect any hardware issued to employees. The University does not maintain such a policy of monitoring or review with respect to the use of the University Technology by, or electronic communications of, students who are not acting as employees or agents of the University.

3.3 To the extent permitted by law, the University has the right, as owner of the University network and other University Technology, to examine, log, capture, archive, and otherwise preserve or inspect any employee data, messages, and electronic communications of all types stored on, traversing, or transmitted over the University's network and other University Technology. Employees using University Technology, therefore, have no reasonable expectation of privacy with respect to any data, files, emails or other electronic communications or usage, all of which under appropriate circumstances may be subject to monitoring/review as is provided below in Section 9 of this Policy.

3.4 All employees should recognize that electronic communications arenot guaranteed to be fully secure, and that during the ordinary course of the administration of the University Technology, network administrators and IT professionals may inadvertently review, or may be required to view, user messages and files.

3.5 All employees using University technology should also be aware that under certain circumstances, including as a result of lawsuits, subpoenas,

and investigations, the University may be required by law to provide electronic communications or other records or information, including such things as email, data, and other computer files created or received or stored by employees of the University on University Technology, to third parties. The University may review, in its reasonable discretion, such information relating to the proper functioning of the University for internal investigations. Employees are hereby placed on further notice that in certain circumstances, the University, to the extent consistent with law, may turn over such information stored on University Technology to law enforcement authorities if there is evidence of possible violations of law, and may cooperate with law enforcement authorities in connection with the investigation of illegal activities or, to the extent required by law, including the Patriot Act, evidence of terrorist related activities.

3.6 Employees should always ensure that the business information contained in email messages and other transmissions and electronic communications of employees are appropriate, professional, and consistent with University policies generally. Employees shall not compose, transmit, access, or retrieve data via University Technology that contains content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person in violation of any law or University policy.

Examples of unacceptable content may include, but are not limited to, inappropriate sexual comments or pornographic images, racial slurs, inappropriate gender-specific comments, or any other improper comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

3.7 University technology is not to be used by employees for personal activities unrelated to proper University functions, except in a purely incidental and occasional manner, or as expressly authorized by the employee's supervisor. Any such personal use, even if authorized, remains subject to the University's right to monitor and review, to the extent permitted by law by and this Policy (see Section 9, below). Personal use by employees of University Technology (whether or not authorized) is considered to constitute consent by the employee to the University to monitor and review such use without further notice or consent, except to the extent prohibited by law. Personal use of University Technology beyond incidental and occasional use more than a few minutes a day, or pursuant to express authorization, may be grounds for disciplinary action.

3.8 The University further reserves the right to determine policies relating to the retention or purging of records, including electronic data and

communications, and the right in its discretion to delete data, communications, and records stored on University Technology.

4. Portable Computers

4.1 Portable computers (i.e., laptops / notebooks, netbooks, tablets) are, when determined by the University to be appropriate, made available to employees to use when traveling or presenting to groups or as a way to stay in touch with the University while away from campus.

4.2 Costs incurred by the University from damages to or the loss of a portable computer is the responsibility of the employee if the result of intentional damage, improper care, or gross neglect. Employees shall be responsible to report immediately any stolen portable computers to the Public Safety Department and the Office of Information Technology.

4.3 As with all University computers and other University Technology, employees are prohibited from installing unauthorized software or hardware components on University issued laptops. Before installing any software, an employee is required to contact the Office of Information Technology for authorization and to determine that any necessary licensing has been secured. Only the Office of Information Technology may install new software on University owned or leased hardware.

4.4 Confidential, privileged, or sensitive information about the University should never be permanently stored on a portable computer. Any such information shall be transferred to the University's network where the data is secured and regularly backed-up.

4.5 In the event that the employee becomes aware that the security of a University laptop has been breeched or compromised, the employee shall immediately advise the Office of Information Technology and Department of Public Safety.

4.6 As with all University Technology, the University reserves the right to inspect and monitor University laptops used by employees in accordance with the conditions and procedures set forth in Section 9 of this Policy.

5. Abuse and Excessive Use

5.1 Abuse by employees of University technology in violation of law or University policies, including this Policy, will result in disciplinary action or termination of employment. To the extent provided by law, employees may also be held personally liable for any losses caused by violations of this Policy.

5.2 The following are examples of behaviors and activities by employees that are prohibited by this Policy and can result in disciplinary action or termination of employment:

a. Engaging in any activities that would use excessive system resources or overwhelm the natural capacities of the technology infrastructure. (Chain letters, the excessive downloading of large files, downloading of any software or programs, or the use or downloading of web-crawlers, streaming videos, or music without authorization are prohibited.)

b. Solicitation in violation of University policies regulating solicitation or sales by employees of others (employees or non-employees) using University Technology, including for commercial ventures, religious or political causes, outside organizations, or other non-business matters.

c. Using University Technology for any sort of gambling.

d. The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material while using University Technology.

e. Sending or posting discriminatory, harassing, or threatening messages or images or sending or posting messages that defame or slander other individuals in violation of law or University policies (including the Harassment Prevention Policy).

f. Participating in the viewing or exchange or downloading of pornography or obscene materials. (See Section 6 below.)

g. Using University Technology for personal gain or engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions.

h. Stealing, using, or disclosing someone else's account code or password without authorization.

i. Violating copyright law by copying, pirating, or downloading software and electronic files without permission or failing to observe licensing agreements.

j. Sending or posting confidential material, trade secrets, privileged communications, or proprietary information of the University to

unauthorized third parties outside of the University or to unauthorized recipients within the University.

k. Jeopardizing the security of University Technology or attempting to break into the computer system of another organization or person using University Technology.

l. Refusing to cooperate with a security investigation by the University.

m. Passing off personal views as representing those of the University.

n. Sending anonymous email messages.

o. Engaging in any illegal activities using University Technology.

p. Using University Technology for personal purposes in excess of the generally permitted occasional or incidental use noted above, (not to exceed a few minutes a day except to the extent expressly authorized by the employee's supervisor).

q. Installing unauthorized software on University hardware or systems.

r. Installing unauthorized hardware into the University networks or systems.

6. No Harassment

6.1 It is University policy that all individuals within the University community have the right to an environment free from any type of discrimination, including any form of unlawful harassment. The University prohibits the use of University Technology by employees in a manner that violates the University's Harassment Prevention Policy. (Refer to the Lincoln University Harassment Prevention Policy for further detail.)

6.2 It is not the intent of this Policy to unduly inhibit the expression of ideas or to use any methods that would infringe on an individual's right to free speech. This Policy is intended to create a working environment that promotes respect and dignity for others and the protection of legitimate University interests while reasonably striking a balance with the interest of employees' freedom of expression.

7. Security Controls

7.1 Information technologies are protected and controlled through the use of account codes and passwords and in some instances filters and protective software. University Technology users may not share their Lincoln computer accounts or passwords, and may not use the accounts or passwords of others. Violations of this by employees may result in disciplinary action.

7.2 Security controls on University Technology are established to protect individual privacy and to safeguard University information and physical assets. All members of the University community must respect these controls, refrain from attempting to circumvent them, and must promptly report to the Chief Information Technology Officer or their immediate supervisor violations of such Technology security controls as they are discovered.

8. University Policy on Institutional Monitoring or Review of Employee Electronic Communications or Files

8.1 University Technology, including computer equipment and systems, and data and communications and files created, sent, received or stored therein are the property of the University. To the extent permitted at the time by law, the University reserves the right to monitor and review any and all aspects of the University's computer systems and data, communications and files of employees stored on University Technology, at any time, without notice, and without the employee's permission. Lincoln similarly reserves the right to monitor and review Internet traffic of employees, including the history of sites visited, and retrieve and read any data composed, sent, or received through its University's online connections and stored in University Technology.

8.2 Accordingly, no University employee should have any expectation of privacy vis-à-vis the University in any message, file, image, or other electronic communications of employees created, sent, saved, transmitted, retrieved, received, or stored by use of the University's Technology.

8.3 The University will not ordinarily monitor or review the content of electronic communications or computerized files of its employees except under certain special circumstances. Monitoring and review of electronic communications of computerized files may only be performed by University employees authorized by the President or designee and Chief Human Resources Officer. Other employees must not impede this monitoring, review, or attempt to monitor or review the communication of others. In this context, "electronic communications" includes, but is not limited to, email and computer files of employees transmitted over the

University network or stored on University's computer system and equipment or other University Technology.

8.4 Examples of special circumstances when monitoring or review of employee electronic communications may occur include, but are not limited to, the following:

a. Communications or files targeted by orders of a court of law, subpoena, or proper discovery demands.

b. Supervisor and/or internal audit reviews of University systems or records.

c. Electronic communications or files that have been inadvertently exposed to IT staff who are in good faith working to upgrade systems or correct technical issues. When IT staff inadvertently becomes aware of potentially illegal or improper content in communications or files, they are required to report what they have seen to appropriate authorities at the University. Otherwise, however, the University expects IT staff to treat inadvertently viewed electronic communications of University employees (or other users) as confidential and not subject to disclosure to anyone (including within the University) without authorization by the President or the President's designee.

d. Security testing and similar routine administrative functions by the IT staff and investigations of attempted improper access (i.e. "hacking") into University systems by unauthorized persons.

e. Investigations into allegations of violations of law or University policy.

f. An urgent need for access to University business documents when an employee is unavailable.

g. Reviews of documents released to third parties, including but not limited to disclosures in accordance with a court order or subpoena or discovery request, to determine whether the communications or files must be disclosed and/or whether they contain and confidential or privileged information of the University. Such situations will be specifically reviewed by and authorized by the President, the President's designee, or by the Vice President responsible for the affected employee.

9. Severability/Consistent with Law

9.1 Nothing in this Policy shall not be construed to require the disclosure by the University to third parties of any confidential or privileged communications.

9.2 In the event that any provision of this Policy is ever determined to be inconsistent with any law, the applicable law shall prevail and that specific portion of the Policy shall be considered to be severed from the Policy, but the rest of this Policy shall remain in force until further action is taken by the University to amend this Policy.

10. Violations of this Policy

10.1 Violations of this Policy should be reported to the immediate supervisor, Division Vice President, Chief Information Technology Officer, Director of Human Resources, or to any member of management.

10.2 Any violation by employees of this Policy or any laws related to the use of information and communication technologies will be subject to disciplinary action or termination of employment.

References

Lincoln University Harassment Prevention Policy

Questions regarding this policy may be addressed to:

The Office of Human Resources
Lincoln University
1570 Baltimore Pike
Lincoln Hall – 4th Floor
Lincoln University, PA 19352
484-365-8059