POLICY GOVERNING ACCESS TO AND USE OF UNIVERSITY TECHNOLOGY RESOURCES

I. Introduction

Computers, network systems, and other associated technologies offer powerful tools for creating, communicating, and managing data, and for a host of other activities. Taxpayers, students, and other groups providing sources of funding that support technology resources at the University expect that these assets will be used in support of the University's mission of research and creative activity, teaching and learning, and service.

The University generally does not monitor or restrict the content of material transmitted, stored, or posted on University-owned computers, but reserves the right to limit or remove access to its networks and to material posted on its computers, when applicable University regulations, contractual obligations, or state or federal laws are violated. Individuals who use University systems and email for any work-related or personal matters do not acquire an absolute right of privacy for data, documents and communications transmitted or stored on University technology resources.

II. Scope

This policy applies to all users of University technology resources irrespective of whether those resources are accessed from on-campus or off-campus locations. This policy applies to current faculty (including post-doctoral fellows), staff, volunteers, currently enrolled students (including undergraduate, graduate, and non-degree), retired faculty and staff, spouses of faculty or staff who become deceased while employed by the University, certain persons affiliated with external agencies collaborating with the University, and any other person employed by the University or who is authorized to use University resources.

III. Technology Users' Privileges and Responsibilities

A. The University grants technology resources access to an individual solely for the grantee's own University mission-related use.

B. All users are expected to exercise common sense and decency, including due regard for the rights of others, with respect to the public technology resources.

C. Technology resources may not be used in a manner that violates the law, for private commercial activities that are not approved by the University, for personal private

gain, or for political campaigning and similar activities that are inconsistent with the University's tax-exempt status.

D Incidental personal use is an accepted and appropriate benefit of being associated with the University's technology environment. The senior management of each administrative unit is authorized to determine the nature of incidental personal use by members of the unit. An employee's supervisor may require the employee to cease or limit any incidental personal use that hampers job performance or violates University policy.

E. Access may be limited or revoked if an individual misuses resources or violates applicable University policies or state or federal laws.

F. The University will handle misuse and abuse of technology resources in accordance with existing University policies and procedures, or state, or federal laws. The University may also take legal action against individuals or entities involved in misuse or abuse of University technology resources.

IV. Confidentiality

A. In general, information stored on computers is considered confidential, whether protected by the computer operating system or not, unless the owner intentionally makes that information available to other groups or individuals. The University will assume that the computer users wish the information they store on central and campus shared computing resources to remain confidential. Requests for disclosure of confidential information will be reviewed by the senior administrator of the computer system involved. Such requests will be honored only when approved by the University officials authorized by the University, or when required by state or federal law. Except when inappropriate or impractical, computer users will receive prior notice of such disclosures.

B. Free expression of ideas is central to the academic process. The University acknowledges the importance of the diversity of values and perspectives prevalent in an academic institution, and is respectful of freedom of expression of ideas. The University does not condone censorship nor does it endorse the inspection of electronic files or monitoring of network activities related to individual activities.

C. However, legitimate reasons for persons other than the account holder to access computer files, computers, or network traffic, or to disclose data to third parties, are:

1. to ensure the continued integrity, security, or effective operation of University systems;

2. to protect user or system data;

3. to ensure continued effective departmental or operations;

4. to ensure appropriate use of University systems;

5. to satisfy a legal obligation; or

6. in health and safety emergencies.

D. In any case where it becomes necessary for persons other than the account holder to access computer files or computers or network traffic for one or more of the purposes outlined above, all reasonable attempts will be made to limit the access the related purpose and to preserve confidentiality of any personal identifiers.

V. Security

A. Users should be aware that although the University takes reasonable security measures to protect the security of its computing resources and accounts assigned to individuals, the University does not guarantee absolute security.

B. The University will help users of its central and campus shared computing resources protect the information they store on those resources from accidental loss, tampering, or unauthorized search, or other access. In the event of inadvertent or non-malicious actions resulting in the loss of or damage to information, the invasion of the user's identity or privacy, the University technology department will make a reasonable effort to mitigate the loss or damage.

C. The University will provide an industry-standard level of system security on University maintained systems. Users are responsible for properly safeguarding the technology under their control, specific to files associated with their computer accounts.

D. Users may request that arrangements be made to protect information stored on such resources. These requests will be honored at the discretion of the unit that manages the resources.

VI. System Administrators Responsibilities

A. Both University and departmental system administrators of computing resources are responsible for the security of information stored on those resources, for making appropriate information on security procedures available to users of those systems, and for keeping those systems free from unauthorized access. Administrators of departmental and individual computing resources shall not implement any policy or procedure that is less restrictive than University requirements.

B. University or departmental system administrators are prohibited from removing any information from individual accounts unless the University system administrator finds that:

1. The presence of the information involves illegality (e.g. copyrighted material, software used in violation of a license agreement, or child pornography).

2. The information in some way endangers computing resources or the information of other users (e.g. a computer worm, virus, or other destructive program).

3. The information is inappropriate, because it is unrelated to or is inconsistent with the mission of the University, in violation of University policy, or is otherwise not in compliance with the legal and ethical usage responsibilities listed in the Fair Use policy.

C. Departmental system administrators (or University system administrators) may access or permit access to the resources described above, if he or she:

1. Has written (verifiable email or paper) permission from the individual to whom the account or device or communication has been assigned or attributed; or

2. In an emergency situation, has a reasonable belief that a process active in the account or on the device is causing or will cause significant system or network degradation, or could cause loss/damage to system or other users data; or

3. Receives a written request from the senior executive officer of a department to access the account of a staff or faculty member who is deceased, terminated, or is otherwise incapacitated or unavailable for the purposes of retrieving material critical to the operation of the department.

D. University system administrators may access or permit access to the resources described above, if he or she:

1. Receives a legal order and/or subsequent written direction from University Counsel;

2. Receives a written authorization, including an explanation of reasonable belief, from the appropriate executive vice president or Provost, for situations where there is reasonable belief that the individual to whom the account or device is assigned or owned has perpetrated or is involved in violations of university policy using the accounts or device in question; or

3. Receives a written request from the Dean of Students, including an explanation of reasonable belief, for situations where there is a reasonable belief that a student to whom the account or device is assigned or owned has perpetrated

or is involved in illegal activities, or is in violations of University policy using the accounts or device in question.

VII. Appeals

Users who wish to appeal such removal of information may do so through the relevant administrative process appropriate to the status of the user (i.e., staff, faculty, student).

VIII. Misuse and Abuse of Technology Resources

A. In the event that University officials are notified of alleged misconduct or illegal activity on the part of a member of the University community, after consultation with Human Resources and Legal Counsel, contents of an individual's e-mail, other computer accounts, office computer, or network traffic may be copied and stored to prevent the destruction and loss of information, pending formal review of that material.

B. Except when inappropriate or impractical, efforts will be made to notify the involved individual prior to accessing the computer account or device, or before observing network traffic attributed to them. Where prior notification is not appropriate or possible, efforts will be made to notify the involved individual as soon as possible after the access.

C. The Kentucky Open Records Act requires that public records be made available to any citizen who requests them, subject to specific state or federal exemptions (e.g. KRS 61.878 and FERPA).

D. Stored computer information, voice and data network communications, and personal computers may not be accessed by someone other than the person to whom the computer account in which the information has been stored is assigned, or from whom the communication originated, or to whom the device has been assigned, outside of the provision of the policy. This policy covers:

1. Data and other files, including electronic mail and voice mail, stored in individual computer accounts on University-owned centrally-maintained systems;

2. Data and other files, including electronic mail and voice mail, stored in individual computer accounts on systems managed by the university on behalf of affiliated organizations;

3. Data and other files, including electronic mail or voice mail, stored on personally-owned devices on University property (e.g., residence hall rooms);

4. Data and other files, including electronic mail or voice mail stored on University-owned computers assigned to a specific individual for their use in support of job functions; and,

5. Telecommunications (voice or data) traffic from, to, or between any devices described above.

IX. Principles Governing Use of Technology Resources

A. User access is granted to an individual and shall not be transferred to or shared with another without explicit written authorization by the Vice President for Information Technology, a designee, or the appropriate system administrator.

B. User access to technology resources is contingent upon prudent and responsible use including following appropriate security measures.

C. The user shall not use technology resources for any illegal or unauthorized act; in particular, the user shall not use technology resources to violate any state or federal laws or any of the regulations specified in the Governing Regulations and Administrative Regulations, the Student Rights and Responsibilities handbook (Code of Student Conduct), the Rules of the University Senate, the Faculty Code, the University System Faculty Handbook, or the Staff Handbook.

D. The user shall not use technology resources for any commercial purpose without prior written authorization from the Vice President for Information Technology, or a designee.

E. Technology resources shall be shared among users in an equitable manner. The user shall not participate in any behavior that unreasonably interferes with the fair use of technology resources by another.

F. Technology resource users can facilitate computing in the University environment in many ways, including:

1. Regular deletion of unneeded files from one's accounts on central or shared machines.

2. Refraining from overuse of connect time, information storage space, printing facilities, or processing capacity,

3. Refraining from overuse of interactive network capacity.

X. Violations

A. Examples of Violations

Violations of these principles or any attempt to violate these principles constitute misuse. Violations include, but are not limited to:

1. Sharing passwords or acquiring another's password without prior written authorization from University Technology Services or the appropriate system administrator.

2. Unauthorized accessing, using, copying, modifying, or deleting of files, data, userids, access rights, usage records, or disk space allocations.

3. Accessing resources for purposes other than those for which the access was originally issued, including inappropriate use of authority or special privileges.

4. Copying or capturing licensed software for use on a system or by an individual for which the software is not authorized or licensed.

5. Use of technology resources for remote activities that are unauthorized at the remote site.

6. Causing computer failure through an intentional attempt to "crash the system," or through the intentional introduction of a program that is intended to subvert a system, such as a worm, virus, Trojan horse, or one that creates a trap door.

7. Intentional obscuring or forging of the date, time, physical source, logical source, or other header information of a message or transaction.

8. Interception of transmitted information without prior written authorization from University Technology Services or the appropriate system administrator.

9. Failure to protect one's account from unauthorized use (e.g., leaving one's terminal publicly logged on but unattended).

10. Violation of priorities for use of technology resources as established by an individual facility within the University system.

11. Excessive use of university technology resources, especially when it impedes the mission-related activities of other users, or adversely affects system availability or performance.

B. Response to Violations

Violation of this policy shall result in action by the appropriate University office or agency. Violations of KRS 434.840 (Kentucky statutes dealing with unlawful access or use of a computer) shall be referred to the Commonwealth Attorney or the police for investigation and/or prosecution. Similarly, violations of 18 U.S.C. Sec.1030 (Federal

laws dealing with unlawful access or use of a computer) shall be referred to the Federal Bureau of Investigation.

C. University Sanctions

University sanctions are imposed by the appropriate University authority and may include, but are not limited to, limitation or revocation of access rights and/or reimbursement to the University for the technology and personnel charges incurred in detecting and proving the violation of these rules, as well as from the violation itself. Reimbursement may include compensation for staff work time related to the violation and for archiving information related to the incident. Disciplinary actions as defined in the Code of Student Conduct, Human Resources Policy and Procedures, and Administrative and Governing Regulations, and University Senate Rules may also include any combination of disciplinary action, or civil or criminal liability. The usual rights and privileges of appeal apply.

D. Investigation and Review of Charges

1. When the Vice President for Information Technology, a designee, or the appropriate university system administrator has reason to believe that a violation may have occurred, he or she may initiate an investigation and suspend technology privileges for the individual(s) involved, pending further investigation.

2. If significant University sanctions are imposed, such action, together with an explanation of the causal events, shall be reported by the Vice President or the appropriate system administrator to the Dean of Students' Office, in case of students; or to the Provost or appropriate executive vice presidents' offices, for all others.

3. In cases where a user's technology privileges are limited or revoked, a user may request a review of the action. The review shall be conducted by University Technology Services according to established procedures.

GLOSSARY

Access right: permission to use a University technology resources according to appropriate limitations, controls, and guidelines.

Commercial purpose: a goal or end involving the buying and/or selling of goods or services for the purpose of making a profit.

Technology resource: any computing or network equipment, facility, data, or service made available to users by the University.

Data: a representation of facts, concepts, or instructions suitable for communication, interpretation, or processing by human or automatic means.

Disk space allocation: the amount of disk storage space assigned to a particular user by University Technology Services or the appropriate system administrator.

Eligible access: Persons having the following affiliations with the University are eligible to access and use University technology resources:

(1) Current faculty and staff, including post-doctoral fellows;
(2) Currently enrolled students (including undergraduate, graduate, and non-degree students);
(3) Retired faculty and staff;
(4) Spouses of faculty or staff who become deceased while employed by the University;
(5) Certain persons affiliated with external agencies collaborating with the University; and,
(6) Any other person employed by the University or authorized to use University resources.

For groups 3, 4 and 5 access is generally limited to electronic mail. If resources become constrained, this practice will be reviewed and may be restricted or eliminated in favor allocating required resources to uses by active faculty, students, and staff. Unless eligible though another affiliation, alumni of the University are not eligible to access and use university technology resources

Fair use: use of technology resources in accordance with this policy and with the rules of an individual University facility; use of technology resources so as not to unreasonably interfere with the use of the same resources by others.

File: a collection of data treated as a unit.

Incidental personal use: is the use of technology resources by members of the University community of support of activities that do not related to their university employment or studies or to other activities involving and approved by the university. Examples include use of email to send personal messages to friends, family, or colleagues, including messages relating to one-time minimal sales or purchase transactions, and occasional use of the web to gain information about personal interests. If personal use adversely affects or conflicts with university operations or activities, the user will be asked to cease those activities. All direct costs (for example, printer or copier paper and other supplies) attributed to personal incidental use shall be assumed by the user.

Information Technology Resources: information technology devices (personal computers, printers, servers, networking devices, etc.) involved in the processing, storage, and transmission of information.

Inappropriate use of authority or special privilege: use of one's access right(s) or position of authority in a manner that violates the rules for use of those privileges as specified by the Vice President for Information Technology, a designee, or the appropriate system administrator.

Non-mission-related activities: If the user's senior management or academic sponsor determines that the excessive use does not serve the mission of the University, the user will be notified to cease the activity.

Password: a string of characters that a user shall supply to meet security requirements before gaining access to a particular technology resource.

Prudent and responsible use: use of information technology resources in a manner that promotes the efficient use and security of one's own access right(s), the access rights of other users, and University technology resources.

Remote activity: any technology action or behavior that accesses remote site facilities via a University information technology resource.

Remote site: any information technology/network equipment, facility or service not part of, but connected with, University technology resources via a communications network.

System administrator: any individual authorized by the Vice President for Information Technology, the Provost or appropriate executive vice president, or a designee to administer a particular technology hardware system and/or its system software.

Transmission: the transfer of a signal, message, or other form of intelligence from one location to another.

Unauthorized act: with the exception of technology actions or behaviors permitted in this policy, any such act performed without the explicit permission of the Vice President for Information Technology, a designee, or the appropriate system administrator.

Usage record: information or data indicating the level of usage of information technology resources by a particular user.

User: an individual, including student, faculty, staff, or individual external to University, who uses University technology resources.

Userid: a character string that uniquely identifies a particular user to a University technology resource.