Knox College Policy on Acceptable Use of Information Technology Resources

I. General Principles

Access to information technology resources owned or operated by Knox College is a privilege and imposes certain responsibilities and obligations, and is granted subject to College policies, and local, state, and federal laws. Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment. It does not bring the reputation of the College into disrepute.

Information technology resources are defined as all computer-related equipment, computer systems, software/network applications, interconnecting networks, facsimile machines, voice-mail and other telecommunications facilities, as well as all information contained therein owned or managed by Knox College.

Computers, networks, and communications equipment utilized by Knox College -- like other property of the College -- are provided to support the educational mission of the College. Personal use by students also is expected as part of the residential learning program. This policy applies to all members of the Knox College community -- faculty, staff, students, alumni, and retirees. Faculty and staff, however, differ from students in a few important ways. The primary purpose of the equipment (or "business use") may include academic, administrative, research, co-curricular, or

other uses consistent with the position of the individual member of the faculty or staff, and may vary widely. Faculty and staff may make personal use of the equipment. However, the following points apply:

- Personal use should not interfere or conflict with business use.
- The loading of games or other non-business related software that might interfere with the normal operation of one's computer is prohibited.
- The use of College systems by faculty and staff for partisan political purposes is prohibited in order to maintain and not jeopardize our charitable tax-exempt status.
- As an employer and the owner of the network and e-mail system, the College has the right and discretion to access and copy employee e-mail and other information stored on College owned equipment. As a policy, the College respects the privacy of faculty and staff files, and will limit such access as described in the section on "Electronic Privacy" below.
-

II. Guidelines

In making acceptable use of resources, the user must:

- Protect his/her College network user ID and system from unauthorized use. The user is responsible for all activities that originate from the user's College network user ID.
- Access only information that is his/her own, that is publicly available, or to which the user has been given authorized access.
- Use only legal versions of copyrighted software in compliance with vendor license requirements that have been reviewed and approved by the College.
- Be considerate in the use of shared resources. The user must refrain from monopolizing systems, overloading with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.
- Respect the privacy of other users.
- Respect intellectual property rights (e.g., as reflected in licenses and copyrights). Please also see the College's "Policy on Intellectual

Property Ownership” in the Faculty *Handbook*, as well as the “Guidelines for Fair Use of Copyrighted Material.”

In making acceptable use of resources, the user must NOT:

- Access the College's network using another user's network ID and password, or access another user's files or data without permission.
- Use computer programs to decode passwords or access control information.
- Attempt to circumvent or subvert system or network security measures.
- Engage in any activity that is intentionally harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to College data.
- Use College systems for commercial purposes, such as using electronic mail to circulate advertising for products or in any other way jeopardize the College's charitable, tax-exempt status.
- Make or use illegal copies of copyrighted software, store such copies on College systems, or transmit them over College networks.
- Use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited or anonymous messages, by repeatedly sending unwanted mail, or by using someone else's name or user ID.
- Waste computing resources or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings.
- Use the College's systems or networks for personal gain; for example, by selling access to your user ID or to College systems or networks, or by performing work for profit or personal financial gain utilizing College resources in a manner not authorized by the College.
- Use College systems or networks for material or purposes that would violate College policies.
- Use College systems or networks for material or purposes that would violate state or federal law.
- Engage in any other activity that does not comply with the General Principles presented above.

III. Information Disclaimer

Knox College disclaims any responsibility and/or warranties for information and materials residing on non-college systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of Knox College, its faculty, staff, students, or trustees. Individuals using computer systems owned by Knox College do so subject to applicable laws and College policies.

IV. ID and Passwords

Privileges to access College computers, systems, networks, and communications are tailored to individual needs and responsibilities and are assigned via a unique user ID. Authentication is required at the time of access through the use of passwords or authorization codes.

The owner of a user ID is accountable for its use. It is the ID owner's responsibility to protect the integrity of accessible systems and preserve the confidentiality of accessible information as appropriate.

- Passwords should be managed solely by the owner of the user ID.
- Passwords should remain confidential.
- Passwords should be changed periodically and any time there is reason to suspect a password has been compromised.
- Passwords should be composed so they are not easily guessed:
    - They should not easily be associated with the ID owner such as the ID itself, family or pet names, nicknames, phone numbers, etc. Deliberate misspellings of combined words are often a good choice.
    - Previously used passwords should not be reused.
    - Words in (even unabridged) dictionaries or other character strings found in available lists should be avoided.
    - Passwords should never be displayed, printed or otherwise recorded in an unsecured manner.

V. Sensitive Areas of Research

The College recognizes that from time to time individuals may engage in areas of research that might be sensitive, legally questionable, or might otherwise appear to violate law or College policy. In order to protect themselves and the College, anyone who contemplates that their research may be considered suspect in any way should notify the Vice President of Academic Affairs/Dean of the College. Instructors are encouraged to consult the College's Institutional Review Board and the policy regarding "Investigations of Allegations of Research Misconduct" (Appendix E of the *Faculty Handbook*).

VI. Electronic Privacy

The College respects the privacy of the members of the College community: faculty, staff, and students. However, while the College will attempt to safeguard that privacy, the College cannot guarantee that privacy will be absolute.

- By its nature electronic communication leaves records or logs of information that can be used to trace problems.
- Some of these logs are --by the nature of the systems -- subject to review by any user of certain systems.
- Transmitted information, such as e-mail messages, can easily be forwarded and copied by recipients, and can (with specialized equipment) be read in transit.
- Personal systems attached to the network may have all or part of their data publicly available. Even data that is password protected may be available if the password is too easily "hacked."
- Files stored in shared disc storage and on College servers are backed up regularly. This means that information deleted by an individual may continue to be accessible in some form.

The College places a high value on privacy and recognizes its critical importance in an academic setting. There are nonetheless circumstances in which, following carefully prescribed processes, the College may determine that certain broad concerns outweigh the value of a user's expectation of privacy and warrant College access to relevant IT systems without the consent of the User. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

A. Non-Investigative Access

In the normal course of working with the College's networks and computers (e.g., routine maintenance, replacing a hard drive, analyzing abnormally high usage of the network, etc.), Information Technology Services staff will come across and see information stored on College owned equipment, as well as on personal equipment that is connected to the College network. Unless there are suspected violations of law or College policy, the staff will respect the privacy of the individual.

The College does not, as a rule, monitor the content of materials transported over the College's network resources or posted on College-owned computers and networks, but reserves the right to do so. The College reserves the right to copy and examine any files or information residing on College systems allegedly related to unacceptable use. It also reserves the right to protect its network from systems and events that threaten or degrade operations.

In accordance with state and federal law, the College may access all aspects of IT systems, without the consent of the user, in the following circumstances:

- When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT system; or
- When required by federal, state, or local law or administrative rules; or
- When, during the course of non-investigative access, Information Technology Services staff discover artifacts which may indicate violation of law or College policy has occurred, additional access or inspection may be performed to produce evidence related to the misconduct or violation. If reasonable grounds exist to suspect such violation, the procedures in Section B (following) will apply; or
- When such access to IT systems is required to carry out essential business functions of the College; or
- In connection with the preservation of public health and safety and to ensure the privacy of protected or confidential information.

B. Investigative Access

Investigative access without the consent of the user will occur only with the approval of the President (for any user), Vice President of Academic Affairs/Dean of the College (for faculty and Academic Affairs staff users), the Vice President for Finance and Administrative Services (for staff users), the Vice President for Student Affairs (for student users), or their respective appointees, except when an emergency entry is urgently needed to preserve the integrity of facilities or to preserve public health and safety. The College, through the Chief Information Officer or designated appointee, will log all instances of investigative access without consent. Information Technology Services staff will also log any emergency entry within their control for subsequent review by the Vice President of Academic Affairs/Dean of the College, Vice President for Finance and Administrative Services, or Vice President for Student Affairs.

User Access Deactivation

In addition to accessing the IT systems, the College may deactivate a user's IT privileges, whether or not the user is suspected of any violation of this policy, when necessary to preserve the integrity of facilities, user services, or data. Information Technology Services staff will attempt to notify the user of any such action.

Use of Security Scanning Systems

By connecting privately owned personal computers or other IT resources to the College's network, users consent to College use of scanning programs (e.g., antivirus, security/compliance agent, operating system updates and patches) for security purposes on those resources while attached to the network.

VII. Enforcement

The College considers any violation of these acceptable use principles or guidelines to be a serious offense. Violators are subject to disciplinary action as prescribed in the Student Handbook, the Faculty Handbook, Employee policies, or as may be adopted by the College.

A. Complaints of Alleged Violations

An individual who believes that he or she has been harmed by an alleged violation of this policy may file a complaint in accordance with established college procedures (including, where relevant, those procedures for filing complaints of sexual harassment or of racial or ethnic harassment) for students, faculty, and staff. The individual is also encouraged to report the alleged violation to the Vice President for Information Technology Services/Chief Information Officer, who must investigate the allegation and (if appropriate) refer the matter to College disciplinary and/or law enforcement authorities.

B. Reporting Observed Violations

If an individual has observed or otherwise is aware of an alleged violation of this policy, but has not been harmed by the alleged violation, he or she may report any evidence to the Chief Information Officer, who must investigate the allegation and (if appropriate) refer the matter to College disciplinary and/or law enforcement authorities.

C. Disciplinary Procedures

Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the College By-Laws, the Faculty Handbook, the Staff Handbook, the Student Handbook, and other applicable materials.

Information Technology Services staff may be asked to participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. Moreover, at the request of the appropriate disciplinary authority, the Information Technology Services staff is authorized to investigate alleged violations.

A. Penalties

Individuals found to have violated this policy may also be subject to penalties provided for in other College policies and practices dealing with the underlying conduct. Violators may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The applicable disciplinary authority in

consultation with the Chief Information Officer shall determine the appropriate penalties.

B. Legal Liability for Unlawful Use

In addition to College discipline, users may be subject to criminal prosecution, civil liability, or both for unlawful use of any Knox College IT system.

C. Appeals

Users found in violation of this policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures. Appeals should be directed to the appropriate Vice President.

Adapted with permission from the Acceptable Use Policy of the Virginia Polytechnic Institute.

Approved by President's Council on February 16, 2016.