INTRODUCTION

In October 1999, the Cottey College Board of Trustees adopted the Strategic Technology Plan. In this document, information technology is defined as:

> Information technology at Cottey College is an infrastructure that directs the use of equipment, systems, and human resources to produce information to enable the College to accomplish its purposes. This infrastructure requires a resource base of hardware, software, databases, staffing, network configurations, and telecommunication devices for the teaching, learning, and support services necessary to further the College's mission and goals.

The Strategic Technology Plan identifies goals for the development of technology policies. The following policy establishes legitimate and proper use of the computing resources and network services of Cottey College, while respecting academic inquiry and freedom of expression. The policy is consistent with the College's Mission and Goals and the College Honor Code: integrity of one's word, intellectual and academic honesty, and respect for and consideration of others and their property.

Academic Computing and Administrative Computing Services manage the College's computing resources and data to further the purposes of the College. As property of the College, computing resources exist for and are intended to support administrative, instructional, research, and communication activities of all directly affiliated with the College. Computing resources include, but are not restricted to, the following:

- Campus Computing Network
- Wireless Network
- Fiber-optic and Cable Networks
- Internet Servers
- Lab Facilities
- Electronic Mail
- Internet Services
- College Workstations and Software
- Institutional Data and Software

SCOPE OF POLICY

Unless otherwise specified, this policy applies to all faculty, staff, and emeriti (hereinafter referred to as employees), students, and guest users of Cottey College computer networks, equipment, and connecting resources. Administrative departments, academic divisions, and academic departments may develop further computing resource policies congruent with the principles in this policy.

PRIVACY

A reasonable effort is made to provide a secure and confidential environment for computer resources, but no guarantee of privacy is made. Neither using a password nor deleting files should give a user an expectation of privacy regarding any information on or the usage of the College's computing system. Although the College does not routinely monitor computer information and usage, any data--professional or personal--or usage may be examined in the

course of systems administration for maintenance or security purposes, in regard to a policy or legal compliance concerns, audits, or as otherwise needed to protect the reasonable interests of the College.

AUTHORIZED USE OF HARDWARE AND NETWORKS

Employees and Students

Authorization is subject to a College administrator assigning a user name and password, and user agreeing to abide by all conditions contained in this policy. Employees using the College Internet Service Provider resources are subject to all conditions and restrictions listed in this policy, as well as the Cottey College Internet Service Provider User Agreement. (See attached Internet Service Provider User Agreement.) Students are authorized to use Cottey's wireless network to access the Internet after the Cottey College Wireless Network User Agreement has been signed. (See attached Wireless Network User Agreement.)

Guests

Guests are authorized to use computers identified as publicly accessible in the Library. At certain times of the year, Academic Computing or Administrative Computing Services may also authorize guests use of and access to specific other computers on campus.

Guest users of campus computer resources are subject to all conditions and restrictions listed in this policy. All other uses of computer resources by persons other than Cottey employees and students are prohibited.

AUTHORIZED USE OF SOFTWARE AND DATA

Employees

College employees are authorized to utilize data and software installed by the College and located on the computer(s) assigned to the employee, or authorized by the employee's supervisor, for purposes related to the employee's job or as identified in the "Personal Use" section of the policy.

When authorized verbally or in writing by a department director or dean, employees of the College may access certain computer software, department databases, and shared file server folders. In most cases, additional department database and computer use policies will apply to the appropriate and authorized use of specific databases and computer files. Contravening a department's policy, or accessing or attempting to access unauthorized College software or data, violates this policy.

Students

Students are authorized by the College to access College e-mail servers, Web servers, and bibliographic databases. In addition, students are authorized to access assigned network user folders. Students may use data and software installed by the College only on computers they are authorized to use. Use of software on a College-owned computer that is not installed or authorized by the College is prohibited.

Guests

Guests are allowed only to access the following College resources:

- Cottey's Website, www.cottey.edu, and Intranet Web pages that do not require a user name and password.
- Cottey Library bibliographic (card catalog) data.
- Data and software installed by the College on publicly accessible computers.

Guest software user guidelines will be posted at each publicly accessible computer or on bulletin boards in computer labs. Any guest use or attempted use of the College's software or data not described above is prohibited.

ETHICAL USE

The Cottey College Honor Code provides a framework of ethical, responsible, and considerate behavior expected of all employees and students. To act ethically safeguards against abuses and violations of policy, thus preserving access to computing resources.

Users will:

- Abide by federal, state, and local laws.
- Respect the legal protection license, and contractual agreements for software, data, and other on-line information.
- Respect and protect the integrity of information resources, including the hardware and software components of a system.
- Be responsible for personal files and the security of their passwords.
- Understand the use of the Internet is a privilege, not a right, and its resources are provided to support educational activities, such as research and academic inquiry.

COMPUTER LABS

Academic work is the priority in computer labs. All workstations are configured for academic use. Software, directories, or data may not be altered. For that reason, chat messenger services software may not be downloaded.

Work in the labs should be saved to a user's folder or disk. During times of heavy use, the rights of other students should be considered, and personal use of computers limited.

Users will:

- Handle equipment with care.
- Use paper conservatively.
- Refrain from bringing food or drink into the labs.

Suspected violations should be reported to the director of academic computing.

PERSONAL USE

After signing required user agreements, employees and students may use computing resources for limited personal purposes, including e-mail, Internet Web browsing, and word processing, as long as the personal activities do not:

- Interfere with an employee's or student's assigned duties or responsibilities.
- Infringe on the rights of others.
- Disrupt or unnecessarily burden the College's computing or financial resources.
- Violate any other section of this policy.

Because the College cannot differentiate between professional or personal data, personal data is subject to examination as stated in the Privacy section. The College is not required to restore or recover personal data.

COPYRIGHT

The College will not tolerate academic dishonesty (cheating, plagiarism) or intellectual property theft. Federal law applies to all forms of information, and violations of that law are prohibited. Copyright protects "original works of authorship," and copyrightable works include (but are not limited to) literature, music, drama, choreography, sculpture, motion pictures, audiovisual multimedia, software, and sound recordings.

Copyrighted materials may be used if the copyright holder gives permission. Copyright law allows for fair use of works for the purposes of criticism, reporting, teaching, scholarship or research, and for limited reproduction by libraries and archives.

CAMPUS WEB PUBLISHING

Organizations may not use the College logo and seal without written permission of the director of public information. Web supervisors must follow all guidelines as set forth in the Cottey Styleguide.

Without notice, any Internet or Intranet Web page hosted on Cottey servers that does not support the Mission and Goals of the College or exceeds the scope of its original approval may be removed or deactivated. Appeals may be made to the President's Council.

Internet

A distributed arrangement has been established in which the responsibility for authoring and maintaining a collection of Internet Web pages is given to individuals and/or departments. The director of public information determines the structure of the College's Web site.

Web pages that constitute divisional, departmental, or organizational content shall have a faculty or staff member responsible for supervising the Web site's development--including its accessibility, timeliness, and accuracy of information. Supervisors are responsible for ensuring compliance with College policies.

Organization Web sites are for private, noncommercial use only. They may not be used to advertise a business, or to buy, sell, or trade anything, whether for profit or not for profit.

Intranet

Administrative department supervisors or student organization advisors are solely responsible for Intranet layout, design and timely updates. Authors are solely responsible for the content. Supervisors or faculty members may request that new pages be linked to the Intranet.

Technical Services

Administrative Computing Services will assist administrative departments with technical or procedural aspects of Web page creation. Academic Computing will assist faculty with technical or procedural aspects of Web page creation. Faculty/staff advisors may facilitate the creation of Web pages for their student organizations, and will serve as a liaison between the organization and the directors of academic computing and administrative computing services for technical and procedural issues.

SECURITY ISSUES

To maintain system availability, authenticity, and integrity of both the wired and wireless networks, the College reserves the right to do the following while data is in transit on the network or on a hard drive:

- inspect network data;
- scan for and remove viruses;
- back up all College-owned computers.

UNACCEPTABLE USE

Unacceptable use falls into four broad categories. These categories involve network, accounts, harassment and infringement, and commercial activities. Violation of the College's guidelines, MOREnet, MOBIUS, city, state, federal or international laws, rules, regulations, rulings, or orders is prohibited.

Networks

Users may not modify, degrade, or damage computers or the computer network. Examples violating this guideline include, but are not limited to, the following:

- attempting to breach security of internal or external systems;
- knowingly transmitting computer viruses, worms, or rogue programs;
- sending large amounts of e-mail (spamming) to an internal or external system;
- using College computers for activities that unduly increase network load (chain mail, network gaming, or excessive use of chat rooms or file downloads);
- tampering with software protections or restrictions;
- downloading unauthorized software.

Account

Users may not access or use materials without authorization. Examples of violations include, but are not limited to, the following:

- sharing a user ID and password with any person on or off campus;
- sending e-mail from another user's account;
- downloading or sending pornography or obscene material;
- accessing unauthorized data;
- damaging electronic information of others by forgery, alteration, or falsification;
- attempting to obtain privileges to which user is not entitled;
- distributing material that misrepresents the College;
- creating or executing any computer program intended to obscure true identity, bypass or render ineffective security, access control on any system, or examine or collect data from a network;
- effecting or receiving unauthorized electronic transfer of funds.

Harassment and Infringement

Users may not harass or impair the activities of others. Examples of violations include, but are not limited to, the following:

- sending chain or pyramid e-mail;
- changing an individual's password to access his or her account or deny him or her access to the account;
- sending unwanted and repeated communication to annoy, harass, threaten, or intimidate another;
- posting or distributing anything offensive regarding race, color, ethnicity, religion, gender, sexual orientation, age, disability, veterans' status, military service, or any basis protected by law;
- misrepresenting one's identity when sending an e-mail.

Commercial Activity

Cottey College computing resources may not be used to run a business or to advertise goods and/or services. Exceptions are made to students selling items to the College community. Users may make non-profit public service announcements.

ENFORCEMENT

Violators of the Cottey technology policy are subject to loss of access to computing resources, as well as to disciplinary action.

Disciplinary proceedings will take place according to the processes outlined in the Cottey College Manual for Hourly Wage Employees, the Cottey College Manual for Administrative Employees, and the Cottey College Faculty Handbook. Student violations will be considered and treated as violations of the Cottey College Honor Code.

Resource Protection

All cases of non-compliance with this policy will be handled as expediently as possible on a need-to-know basis. Administrative Computing Services will take the immediate and necessary precautions to safeguard the computing resources of Cottey College. Such precautions may include, but are not limited to, the temporary revocation of a user login account or the removal of College-owned equipment from an office or classroom, and should not be construed to be a sanction or a determination of noncompliance.

Non-Compliance Reporting

If a person suspects that someone has violated any portion of this policy, prompt reporting of the situation is critical to maintaining the security of the network and computing resources and preserving any evidence needed to determine if a violation has occurred. The procedure for reporting a possible violation follows. The person who suspects a violation of this policy should refrain from discussing with anyone the reporting of a possible violation.

Staff

A person who suspects that a staff member has violated this policy should immediately contact the staff member's supervisor and, if the supervisor is not known or available, the director of administrative computing services.

Faculty

A person who suspects that a faculty member has violated this policy should immediately contact the vice president for academic affairs and, if the vice president is not available, the director of academic computing.

Student

A person who suspects that a student has violated this policy should immediately contact the director of academic computing services or the director of administrative computing services or the dean of student life.

Guest

Library
A person who suspects that a guest has violated this policy should immediately contact the administrator on duty in the library.

Center for Women's Leadership
A person who suspects that a guest has violated this policy should immediately contact the director of the Center for Women's Leadership, and if the director is not available, the director of administrative computing services.

Other Campus Computers
A person who suspects that a guest has violated this policy should immediately contact the event or facility coordinator, or the director of administrative computing services, or the director of academic computing.

Non-Compliance with the Law

The College will not tolerate the use of computing resources in violation of the law. The College may assist in the investigation and prosecution of any alleged criminal activity involving its computing resources or the College may be compelled by court order or subpoena to access or disclose information on the College's computing resources or network systems. Missouri Revised Statutes 569.095 - 569.099 describe the penalties for tampering with computer data, equipment, and users, which can range from a class A misdemeanor to a class C felony. No employee, student, or guest shall assist in such investigation on behalf of the College or comply with a court order or subpoena seeking College information without prior authorization from the President of the College.