COTTEY COLLEGE TECHNOLOGY POLICY
ACCEPTABLE USE POLICY

The offices of 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, academic, communication, and enrichment activities of all directly affiliated with the College. Computing resources include, but are not limited to:

- ❑ campus computing network;
- ❑ wireless network;
- ❑ fiber-optic and cable networks;
- ❑ Internet servers;
- ❑ lab facilities;
- ❑ email;
- ❑ college workstations and software;
- ❑ institutional data and software.

SCOPE OF POLICY

Unless otherwise specified, this policy applies to all users[1] 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 guidelines in this policy.

PRIVACY

A reasonable effort is made to provide a secure and confidential environment for computing resources, but no guarantee of privacy is made. Users should not assume or expect any right to privacy with regard to use of the College's computing resources or any data stored on or transferred by those resources. Neither using a password nor deleting files should give a user of a connected device[2] an expectation of privacy regarding any information on, or the usage of, the College's network[3]. Although the College does not routinely examine the documents and emails created by individuals, any data[4], professional or personal, traversing[5] or residing on the college's network 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 interests of the College.

[1] Faculty, staff, trustees, and emeriti (hereinafter referred to as employees), students, authorized and unauthorized guests.

[2] Includes College and personally owned computers, tablets, flash drives, cell phones, smart phones, games systems, cameras, and televisions connected locally or remotely to the campus network.

[3] Wireless network, wired network, and college owned computers.

[4] Intranet and Internet web activity (regardless of privacy settings established within a web application), email messages and attachments, audio and video, Internet telephone (Skype, VoIP, iPhone), office telephone, instant messages, mobile device text messages when forwarded to campus email, voice mail, file uploads/downloads.

[5] Moving through servers, network hardware, devices, cables, and wireless signals.

AUTHORIZED USE OF HARDWARE AND NETWORKS

Employees and Students

Authorization is established by a College administrator assigning a user name and password, and user agreeing to abide by all conditions contained in this policy.

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, other specific computers on campus.

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 vice president, 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 software installed by the College only on publically accessible computers in the Library, computer suites, computer labs, and classrooms. Use of software on a College-owned computer that is not installed or authorized by the College is prohibited.

Guests

Guests are allowed to access only 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 data;
- ❑ software installed by the College on publicly accessible computers.

Additional guidelines may 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 and College computing resources is a privilege, not a right, and its resources are provided to support educational activities, such as research and academic inquiry.

COMPUTER LABS

All workstations are configured for academic use. Work in the labs should be saved to a user's folder or flash drive. Academic work takes priority over personal use. Software, directories, or data may not be altered.

Users will:

- ❑ handle equipment with care;
- ❑ use paper conservatively;
- ❑ refrain from bringing food or drink into the labs.

PERSONAL USE

After agreeing to this policy, 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 personal data or college owned data, all 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 prohibits the unauthorized use of copyrighted materials. 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. All users of copyright-protected materials are responsible for ensuring compliance with federal law.

CAMPUS WEB PUBLISHING

Organizations may not use the College logo and seal without written permission of the director of public information. 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.

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.

It is College policy to block access to any device containing college email/documents that has been lost or stolen. Cottey procedures to manage blocked access to devices super cedes carrier procedures. Immediately upon learning of a loss, users are required to report the loss of any device containing college email/documents to Administrative Computing Services or Academic Computing as soon as possible.

To reduce the likelihood of contributing to identity theft, and reduce the likelihood of a breach of security that may compromise the security of personal information , Cottey prohibits employees from storing social security numbers, credit card numbers, other financial account numbers, college passwords, and student/staff ID numbers on any College or personally owned laptop, cell phone, flash drive, or mobile connected device or cloud service, e.g. Dropbox, SkyDrive, Google Drive. Additionally, cloud services for which the College does not have a confidentially agreement should not be used to store unencrypted confidential College documents and FERPA protected student educational records.

This policy is meant to supplement other Cottey policies regarding security and the handling of private information, including student educational records and health records. All authorized users of College computing resources must comply with all other applicable Cottey policies.

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:

- 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.

Accounts

Users may not access or use technology resources without authorization. Examples of violations include, but are not limited to:

- sharing a user ID and password with non-authorized IT personnel[6] ;
- giving your password to your supervisor or coworker so they can process your work while you are absent;
- allowing your spouse or children to use your college issued laptop or desktop computer;
- 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 Inappropriate Conduct

Consistent with Cottey's policies against discrimination and harassment, users may not harass or impair the activities of others. Examples of violations include, but are not limited to, the following:

- cyber-bullying;
- 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;
- changing an individual's password to access his or her account or deny him or her access to the account;
- sending or posting unwanted communication to annoy, harass, threaten, or intimidate another;

[6] Persons working in the Administrative Computing Services, or Academic Computing offices.

- misrepresenting one's identity when sending an e-mail;
- engaging in any illegal activities, regardless of whether the user is aware the at-issue conduct is illegal;
- sending chain or pyramid e-mail.

These examples are not exhaustive and are listed to be instructive of the types of prohibited conduct. Cottey expects all users to maintain the same high standards of professional and ethical conduct when using the College's computing resources that are required in other contexts. The College will not tolerate offensive, discriminatory, or harassing behavior in any context.

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 in the buy/sell/trade web board. Users may make non-profit public service announcements.

ENFORCEMENT

Violators of this policy are subject to loss of access to computing resources, as well as 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. Faculty and staff may be subject to discipline up to and including termination for violations of this policy. Student violations will be considered and treated as violations of the Cottey College Honor Code.

In addition to discipline issued by the College, the College may report illegal activity to the proper authorities, including local, state, and/or federal authorities.

Resource Protection
All cases of non-compliance with this policy will be handled as expediently as possible on a need-to-know basis. IT personnel 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 person who suspects a violation of this policy should refrain from discussing with anyone the reporting of a possible violation. The procedure for reporting a possible violation follows.

<u>Staff</u>
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 or the director of administrative computing services or the vice president for student life.

Guest

A person who suspects that a guest has violated this policy should immediately contact:

In the Library: the administrator on duty in the library.

In the Center for Women's Leadership: 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: 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. Violators are subject to penalties described in current applicable federal and/or Missouri laws.

Investigations

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. However, 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, or vice president for administration and finance, unless prohibited from providing prior notice and/or obtaining authorization by legal process or court order.