Title – Ethical Use Policy

Policy Abstract – The primary aim of the College in providing information and technology resources is to support the educational, instructional, and administrative endeavors of the students, faculty, and staff of the College. It is the intent of the College that all technology resources will be used in accordance with established policies of the College and with any and all local, state, and federal laws, and/or guidelines governing the use of technology and its component parts. Implicit in this is the expectation that all students, faculty, and staff will utilize the technology resources of the College so as not to waste them, abuse them, or interfere with or cause harm to other individuals, institutions, or companies. As is the case with most community resources or facilities, users are expected to balance their own needs against the needs and expectations of other users.

As an academic community, the faculty, students, and staff of Birmingham-Southern College honor intellectual property, respect the privacy of data, and recognize the rights of others. Individuals who access College computing resources incur the responsibility to use those resources in an ethical manner. This policy (or electronic code of ethics) requires all computing activities performed on College equipment to be legal and ethical. The policy is based on adherence to U.S. copyright laws and respect for intellectual labor and creativity as vital elements of the academic enterprise.

Abuse of computing privileges is subject to disciplinary action which may include the loss of computing privileges and other disciplinary sanctions. Flagrant student offenses may be reported to the Social Conduct or Honor Councils, faculty offenses to the Provost, and staff offenses to the Director of Human Resources. An abuser of the College's computing resources may also be liable for civil or criminal prosecution. It should be understood that nothing in these guidelines precludes enforcement under the laws and regulation of the State of Alabama, any municipality or county therein, and/or the United States of America.

Responsible Office – Information Technology, Administration

Official – Anthony Hambey

Contact(s) – Anthony Hambey, 226-4849, ahambey@bsc.edu
Applies To – All employees and students
Effective Date – 2/13/2002
Revision Dates – 9/11/2012 - Placed in the new policy format

11/17/2014 **–** Added clearer definition of technology resources, references to cyberbullying and the handling of student violations of the policy and enhanced e-mail privacy section on list management.

1. **Introduction/Background –** Birmingham-Southern College recognizes the role of information and technology in the academic community and in the larger society. It is the policy of the College to provide all students, faculty, and staff with access to a variety of technology resources and to provide opportunities for all members of the College community to learn to utilize these resources effectively and efficiently. Resources include but are not limited to individual computers, servers, storage devices, media, and personal mobile devices such as phones and tablets, as well as the information, messages, files, and/or data stored on them, and the network systems through which information transmission occurs. Physical access such as but not limited to classrooms, labs, offices, server rooms, equipment closets, underground conduit accesses, and wireless access points are also defined as IT resources covered by this policy. In return, the College expects that technology will be used in legally and ethically appropriate ways, consistent with the Mission Statement of the College. This document explains and defines policies for use of technology resources of the College.

2. **Purpose –** To govern access to College technologies, copyright material, electronic mail operation, and internet use.

3. **Applicable Regulations** – SACS-COC Comprehensive Standard 3.9.2 – Confidentiality of Student Records

Policy Statement –

Access to College Technologies

The electronic resources and technologies of the College are intended for the use of students, faculty, and staff of the College. Use of such resources is limited to these members of the College community. Authorized users are assigned user accounts and passwords by the Department of Information Technology (helpdesk@bsc.edu). Individuals may only use accounts, files, software, and computer resources that are assigned to them under their user accounts. Individual members of the College community are expected to take all reasonable precautions to prevent unauthorized access to files and data and any other unauthorized usage within and outside the College.

It shall be considered a violation of this policy and/or of the BSC Honor or Social Conduct Code to:

- Use someone else's password or log in to someone else's account without authorization, except as may be required for management of system resources.
- Attempt to gain access to computing privileges or resources for which you are not authorized or via means not authorized.

- Give others access (via password or other means) to computing resources to which they are not entitled.
- Use a system for unauthorized purposes, such as advertising for a commercial organization or running a business.
- Read, execute, modify, or delete any file belonging to someone else without explicit permission from the owner, even if the file is unprotected.
- Deliberately destroy, damage, or deface hardware (including, but not limited to system unit, monitor, keyboard, mouse, printer, and cabling.)
- Deliberately introduce worms, viruses, or other software which is designed to damage or destroy software (including, but not limited to applications, operating system, files, etc.)
- Move or install hardware or software without authorization.
- Create, display or transmit harassing, libelous, or threatening messages or materials on the College's computer equipment.
- Attempt to crash a system or exploit weaknesses in security.
- Make unauthorized copies of software that is copyrighted.
- Misuse technology resources in any way that materially impacts on the efficacy of use for others.
- Modify technology resources, utilities, and/or configurations, or to change the restrictions associated with their accounts, or attempt to breach any technology resources security system, whether with or without malicious intent.

The appropriate system administrator may remove or alter as necessary user files that threaten to interfere with the operation of the system or as needed for system maintenance. The system administrator should make every effort to notify the user prior to such action to give the user opportunity to remove such files him/herself. It is recognized that there may be special cases where the threat to the efficacy of system resources is so immediate that prior notification is not possible.

Copyright

Published material is protected by copyright law unless it has been placed in the public domain. The owner of a copyright holds exclusive right to the reproduction and distribution of the copyrighted work. Duplication of any copyrighted material is prohibited unless specifically allowed for in a license agreement. Unauthorized copying of copyrighted material is illegal and punishable under federal law.

Respect for the intellectual work and property of others has traditionally been essential to the mission of educational institutions. As members of the academic community, we value the free exchange of ideas. Just as we do not tolerate plagiarism, we do not condone the unauthorized copying or distribution of protected materials, including software, media, and code.

Only authorized personnel may sign license agreements. Questions about site licenses should be directed to the Information Technology helpdesk.

Illegal copies of copyrighted software material may not be created or used on College equipment, including the LAN.

Individuals are expected to report any violations of this policy and/or problems with the security of any technology resources to the Department of Information Technology (helpdesk@bsc.edu) or the IT Faculty Advisory Committee.

Users should assume all materials on the web are copyrighted unless there is a waiver or disclaimer that is clearly stated by the owner. Copyrighted works on a web page cannot be used without express permission of the copyright owner. Copyright works may include: artwork, articles, cartoons, photographs, music, videos, films, and graphics scanned or used from published works or web sites. It is illegal under Federal law (Title 17 of the US Code, and more recently the Digital Millennium Copyright Act, 105 PL 304) to distribute copyrighted media without a license to do so from the copyright holder. Furthermore, it is a violation of College policy to use the campus network for illegal activities, or in ways that consume capacity and services needed for instruction, research, and other core purposes.

Shareware, or "user-supported" software, is copyrighted software that the developer encourages you to copy and distribute to others. This permission is explicitly stated in the documentation or displayed on the computer screen. The developer of shareware generally asks for a small donation or registration fee if you like the software and plan to use it. By registering, you may receive further documentation, updates, and enhancements. You are also supporting future software development.

Public Domain Software is that software that has been dedicated by the authors to the public domain, which means that the software is not subject to any copyright restrictions. It can be copied and shared freely. Before copying or distributing software that is not explicitly in the public domain, check with the Department of Information Technology (helpdesk@bsc.edu).

The College works with its internet service provider to ensure compliance with all copyright protection laws. When contacted by the service provider regarding failure by students to follow the appropriate laws, the College will utilize its student conduct procedures to sanction students, including the loss of online privileges within the College or service provider's network for an appropriate length of time. Other violations of copyright outlined in this section of the policy by students will be handled through the appropriate student conduct process.

Electronic Mail

As an academic institution, the College honors the principles of individual privacy. These principles extend to privacy of electronic communication. It is expected that individuals who are given access to College computing resources will be responsible in the ethical use of those resources.

The Computer Usage Policies in the Faculty, Staff, and Student Handbooks require all computing activities performed on College equipment to be legal and ethical.

A. General Policies

The following guidelines express the essence of the usage policies for electronic mail. Those who violate any of these policies may be subject to disciplinary action through existing structures for faculty, students, and staff.

It is a violation of the Birmingham-Southern College Computer Usage Policies for Electronic Mail to:

- Forge a signature on electronic mail without consent.
- Send abusive or threatening mail to harass an individual. This includes, but is not limited to sexual, ethnic, religious, racial, sexual orientation, gender-based or other harassment. Threats to personal safety will be reported to Campus Police.
- Send or forward chain letters and/or use the e-mail system for personal advertisements, commercial, political, or solicitation purposes.
- Deliberately flood a user's mailbox with mail.
- Send mail that is deliberately designed to interfere with proper mail delivery and access.
- Attempt to gain access to another person's mail files without his/her consent.
- Deliberately or repeatedly introduce a worm or virus into the College's network environment.

B. Guidelines for Operators, Postmasters, Systems Administrators

Computer systems automatically forward all undeliverable mail to the designated "postmaster." This is a standard feature of mail systems in order to provide the equivalent of the "dead letter" office. When possible, the postmaster will forward mail (from the dead letter office) to one or both of the involved parties.

It is a violation of the BSC Computer Usage Policies for Electronic Mail to:

- Access more of the undelivered mail message body than is necessary to perform postmaster responsibilities.
- Retain, forward, or discuss undelivered mail with others.
- Include the message body of mail in statistical analysis. As part of system management, certain programs may gather statistics on mail usage. These statistics may include the address of the sender, the recipient, length of the message, and date.
- Read, forward, or discuss backup mail files.

- Mail files may be copied as a routine aspect of system backups. This is an automatic process that does not involve any human reading of the files copied. Furthermore, some backups are archived for long-term storage. Such practices are NOT considered a violation of privacy.
- Even with proper permission, messages contained within files shall only be read to the extent needed to assist the user involved.

If a system administrator or postmaster of the BSC System, in the performance of normal duties, comes upon messages whose content are clearly illegal, the computer usage policies extend the right and responsibility to report these messages to the appropriate campus committee or to the Campus Police. Examples might include messages containing illegally obtained credit card numbers, telephone authorization codes, grade reports, criminal conspiracy, or similar items. Such items might be discovered as part of user consultation, dead-letter processing, or other tasks. Random mail browsing of electronic or voice communications shall always be in violation of the BSC Electronic Mail Computer Usage Policies and is never authorized.

C. Privacy

The College will seek to provide a reasonable amount of privacy of electronic mail messages. However, e-mail users should be aware that there is no such thing as a fully confidential e-mail transmission. Sensitive, private messages should not be sent via e-mail. Moreover, violations of the College computer usage policies may jeopardize the guarantee of privacy.

Behaviors that violate these stated expectations regarding email communication will be adjudicated through the relevant and appropriate conduct processes of the College.

A person's user-name and e-mail address are considered to be directory information that can be given to other individuals. Student directory information can be withheld by contacting the Academic Records Office. Employee directory information can be withheld by contacting Human Resources. User-names and e-mail addresses will not be distributed for purposes of mass mailing or advertising.

Any group or individual BSC Alumni wishing to communicate with other alums using BSC maintained email address lists must obtain approval from the Office of Alumni Affairs. Emails must relate to current BSC projects or BSC Alumni events or activities and must support the mission of the College. The email list must be for the specific use requested and cannot be used to promote any other activity unrelated to BSC or in which BSC is not involved. Lists shall not be used for personal benefit or made available for commercial, political, or solicitation purposes.

Internet

The College provides access to the Internet for students, faculty, and staff of the College to further its educational goals and to facilitate the instructional and administrative process. Individuals accessing the Internet through College resources are expected to do so in a responsible and ethical manner and to conform to all established policies. Inappropriate use includes, but is not limited to commercial activities; creating, displaying, or transmitting threatening, obscene, or harassing language and/or materials; cyberbullying (unwanted, aggressive, or potentially demeaning behavior through the use of technology which is often but not necessarily repeated and tends to occur where a power imbalance exists or is perceived to exist); copyright and licensing violations; violation of personal privacy; and acts in violation of federal or state laws. Behaviors that violate these stated expectations regarding the Internet will be adjudicated through the relevant and appropriate conduct processes of the College.

Disclaimers

By using Birmingham-Southern College computing and network resources, each user implicitly accepts all stipulations in this policy and accepts full responsibility for his or /her use and/or misuse of these resources. The College considers each user to be ultimately responsible for his or /her actions, and does not accept liability for the individual. Furthermore, although a reasonable and conscientious effort is made to backup critical data on College resources for disaster recovery purposes, each user is ultimately responsible for backing up his or /her own personal data.

4. **Detail**s – An annual financial audit of the College contains a technology component whereby this is verified each year. Non-compliance with this policy would be reported in the form of comments in the management letter of the audit.

5. **Definitions** – SACS-COC is the Southern Association of Colleges and Schools, Commission on Colleges.

6. **References** – SACS-COC *The Principles of Accreditation 2012 Edition*.