ACCEPTABLE USE OF TECHNOLOGY POLICY

A. Policy

Access to information systems and networks owned or operated by Butler County Community College (BC3) imposes certain responsibilities and obligations and is granted subject to College policies, and local, state and federal laws. Acceptable use is always ethical, reflects academic honesty, shows restraint in the consumption of shared resources and protects all Information Technology (IT) Resources from any unauthorized or unintended use. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance unless covered by legal statutes. The establishment of this policy is to safeguard and protect all information systems, including academic and financial, that support the College's Mission and daily operations.

B. General Guidelines

The Director of Information Technology in conjunction with the Dean of Student Development and/or the Executive Director of Human Resources/Equal Opportunity Compliance Officer is responsible for the enforcement of these guidelines. Any request for use of technology systems other than those identified must receive prior written approval.

In making acceptable use of technology resources users must:

1. use technology only for authorized purposes;
2. protect their user ID and system from unauthorized use. Users are responsible for all activities on their user ID or that originate from their system;
3. access only files and data that are their own, that are publicly available, or to which they have been given authorized access;
4. use only legal versions of copyrighted software in compliance with vendor license agreements;
5. be considerate in their use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, disk space, paper, manuals, or other resources;
6. use only College software unless approval is given by the Director of Information Technology to load other software;

In making acceptable use of technology users must **NOT**:

1. use another person's system, user ID, password, files, or data;
2. use computer programs to decode passwords or access control information;
3. attempt to circumvent or subvert system or network security measures;
4. engage in activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging or deleting files and directories;
5. use College systems for commercial or partisan political purposes, such as using electronic mail to circulate advertising for products or for political candidates;
6. make or use illegal copies of copyrighted software, store such copies on College systems, or transmit them over College networks;
7. waste information technology resources, for example, by intentionally placing a program in an endless loop or by printing excessive amounts of paper;
8. use the College systems or networks for personal gain. For example, by selling access to his/her user ID or to College systems or networks, or by performing work for profit with College resources in a manner not authorized by the College;
9. engage in any other activity that does not comply with the general principles presented above;

10. use computer lab facilities at the College unless enrolled as a current student, employed by the College, or granted permission;
11. install personal equipment on College owned equipment without permission from the Director of Information Technology. These include printers, monitors, LCD displays, keyboards, mice, MagicJacks, IP phones, microphones, and web cams;
12. connect personal equipment to the College network via cabling other than wireless hotspots.

C. Internet Guidelines

1. Internet Access

Access to the Internet from BC3 is a privilege, not a right, and abusers may lose their Internet privileges.

Users must adhere to the following guidelines in addition to the general guidelines listed above:

a. students and employees may access the Internet from designated areas on campus during open lab hours. Class activities take priority over open lab time;
b. access to the Internet should be used for purposes relative to classroom and work assignments and not for recreational purposes, including digital and social media;
c. access to the Internet may not be used for unethical, illegal, or criminal activities;
d. access time may be limited due to the number of people online and equipment availability;
e. downloading files from the Internet to the hard drives of lab PC's is prohibited;
f. students/employees have no reasonable expectations of privacy when using BC3 technology and networks.

2. Digital Media Guidelines

Course content, presentations, and/or lectures shall not be recorded (audio and/or video) without prior knowledge and consent of the instructor, presenter, and/or student. Such recordings are not to be copied, sold, altered, reproduced or distributed without the written consent of the instructor, presenter, and/or student.

Registered students may download digital course materials from their course(s) from within the College's online Learning Management System (LMS) for the purposes of private study or research but may not copy, sell, alter or further reproduce or distribute these materials.

3. Online Testing and Student Identity Verification Guidelines

In compliance with federal regulations (34 CFR 602.17(g)), online instructors shall require students who participate in such classes and/or take exams to verify their identity by using a secure login, a pass code, a webcam, and a microphone; or to take proctored exams.

Students may be required to have photo identification for proctored examinations, which may include video and audio recording with consent of the student. In addition, new or other technologies and practices to assist in verifying student identity may be utilized.

Additional costs for proctoring services or use of other technologies and practices may apply and notice of such costs will be provided to students at the time of registration. Costs may vary.

4. Social Media Guidelines via College Information Systems and Networks

Any online activities, including the use of social media, must not interfere with employee work performance or student academic responsibilities. Employees must adhere to

College policies. Students must adhere to policies set forth by their instructors. Employees and students must ensure that their social networking conduct is consistent with all policies contained in the BC3 Student and Employee Handbooks and the Acceptable Use of Technology Policy and the Mobile Device Usage Policy.

5. For student identity verification purposes, the BC3 student identification photo will be available for view by College Administrators, Staff, and Faculty.

D. General Computer Usage

BC3 technology and networks support the College's Mission, a student-centered learning environment, and provide resources and effective communication for students and employees. The information systems and networks provided must be reliable and secure. Students/employees have no reasonable expectations of privacy when using BC3 information systems and networks.

E. Email Guidelines

Users must be aware of what is acceptable and unacceptable use of the email system at BC3 and any hosting email services. All messages distributed via the BC3 email system are the property of BC3. Electronic communication is instantaneous and permanent. Users should be cognizant of the fact that electronic communication may be forwarded, altered, shared on electronic bulletin boards and/or stored on network systems.

Employees and students are required to use the email address provided to them by BC3 for all correspondence related to the College and for all course-related correspondence between the instructors and their students. Instructors have no responsibility to and are discouraged from accepting and/or responding to an email sent from a student using a non-BC3 email address.

Employees and students are expected to use email with good judgment and to be aware that email messages are not confidential and privacy cannot be guaranteed. Students/employees have no reasonable expectations of privacy when using BC3 technology and networks. Transmitting any identifiable student information via email, including grades, may violate the Family Educational Rights and Privacy Act (FERPA). Instructors must disseminate grades using a secure website such as Blackboard, Colleague, and Lumens. If there is evidence that a user is not adhering to these guidelines, BC3 reserves the right to take disciplinary action, up to and including termination of employment, permanent student dismissal, and/or legal action.

It is strictly prohibited to:

1. send or forward emails that are unnecessary, repetitive, or contain libelous, defamatory, hurtful, offensive, racist or obscene remarks;
2. send or forward emails intended to harass, intimidate, or otherwise annoy another person;
3. forward a message or copy a message or attachment belonging to another user without acquiring permission from the originator first. Be aware that copyright laws apply to all material. For example, it is inappropriate to copy any material owned by others from any source (e.g., cartoons, photographs, articles, poems, graphics scanned from a magazine, etc.) without permission of the owner. Users should assume that all materials are copyrighted unless a disclaimer or waiver is explicitly provided (This is particularly true on the World Wide Web; to include information from some other source on a Web page, link to it, don't copy it. In some cases, even this action may violate copyright of licensing agreements by enabling illegal redistribution of programs or data. If a user is unsure, ask the owner);
4. send unsolicited email messages or chain mail;
5. share your BC3 provided users name and password with anyone;
6. forge or attempt to forge email messages, or disguise or attempt to disguise his/her identity when sending mail.

a. All student email addresses and corresponding account/profile information created by and provided to students by BC3 and any hosting email service must remain unaltered while registered for classes at BC3.
b. Email addresses must match the format specified by BC3.
c. The student's email account/profile information must match that which is contained in the BC3 student management database.
d. Only official name changes and withdrawal/graduation from BC3 will warrant the change of an email address and/or the account/profile information connected to the email account.

7. use the BC3 email system for anything other than legitimate business or classroom purposes.
   a. College use of email – Email is an official means for communications within BC3. Therefore, the College has the right to send communications to students via email and the right to expect that those communications will be received and read in a timely fashion.
   b. Assignment of email addresses – Information Technology assigns all employees and students an official BC3 email address. It is to this official address that the College will send email communications; this official address will be the address listed in the College's Directory for that employee or student.

F. Enforcement

The College considers any violation of acceptable use principles or guidelines to be a serious offense.

1. Individuals or groups who act in a manner contrary to existing policy and accepted standards for computer use are subject to the sanctions and disciplinary measures normally applied to misconduct or lawbreaking. Any violations of the acceptable use of technology must be reported to the Director of Information Technology. A copy of the Information Technology Policy Violation Report is provided in Appendix G and is available online under BC3 Forms.
2. The Director of Information Technology and/or his/her designee will work in conjunction with the Dean of Student Development and/or Executive Director of Human Resources/Equal Opportunity Compliance Officer and investigate the allegations and may disallow network connections by certain computers (even departmental and personal ones); require adequate identification of computers and users on the network; undertake audits of software or information on shared systems where policy violations are possible; take steps to secure compromised computers that are connected to the network; or deny access to computers, the network, and institutional software and databases. The College reserves the right to copy and examine any files or information resident on College systems allegedly related to the unacceptable use. Users are expected to cooperate with investigations either of technical problems or of possible unauthorized or irresponsible use as defined in these guidelines; failure to do so may be grounds for suspension or termination of access privileges.
3. A matter involving students will be referred to the Dean of Student Development. A student who violates any of these guidelines will be subject to disciplinary action up to and including permanent dismissal and possible legal action.
4. A matter involving employees will be referred to the Executive Director of Human Resources/Equal Opportunity Compliance Officer. An employee who violates any of these guidelines will be subject to disciplinary action up to and including termination of employment and possible legal action.

G. Disclaimer

The College will not be responsible for the loss or corruption of user data files of any kind. Use of technology, networks, and facilities at the Butler County Community College shall constitute a full, final, and irrevocable release of Butler County Community College and its agents and employees from any suit, claim, or cause of action arising by virtue of the use of the College's technology,

networks, and facilities, including but not limited to, loss of data or damage to any computer outside of the College due to a computer virus. The user agrees to indemnify and hold the College harmless from any suit, claim, or cause of action arising from the user's abuse or misuse of the technology, networks, and facilities of the College. It is the user's responsibility to backup data at regular intervals and provide computer virus protection for their home and/or office computer.

*Portions of the above Acceptable User Guidelines document were used with the permission of Virginia Tech.
[http://www.va.edu/policies/acceptuseguide.htm1] (16 Oct. 1996).