BRIDGEVALLEY COMMUNITY AND TECHNICAL COLLEGE

OPERATING POLICY

Effective Date	Subject	Number	Page
April 1, 2014	**COMPUTER USE AND ABUSE POLICY**	B-OP-18-14	1 of 4
Supersedes/Supplements:	BC A-OP-12-10 and KV VII-1		
Reference:	West Virginia Computer Crime and Abuse Act		

POLICY STATEMENT

This policy is intended to provide guidelines on proper use for authorized users of BridgeValley Community and Technical College (College) computing and network resources, for effective protection of individual users, and for equitable access to computing resources. In addition, users must comply with the West Virginia Computer Crime and Abuse Act, (http://www.legis.state.wv.us/wvcode/Code.cfm?chap=61&art=1) ARTICLE 3C. WEST VIRGINIA COMPUTER CRIME AND ABUSE ACT. §61-3C-1.

PROCEDURES

Authorized Users

- Are to have valid, authorized accounts and may only use those resources which are specifically authorized.
- May only use their account in accordance with authorized purposes.
- Are responsible for safeguarding their own computer account.
- Shall not let another person use their account, with the exception of authorized computer support personnel or others that may be authorized by the system administrator for a specific purpose.
- May not change, copy, delete, read, or otherwise access files or software without permission of the owner of the files or the system administrator.
- May not bypass accounting or security mechanisms to circumvent data protection schemes.
- May not attempt to modify software installations except when intended to be user customized, as in an academic class on the installed software application.
- May neither prevent others from accessing the system nor unreasonably slow down the system by deliberately running wasteful jobs, playing games, engaging in non-productive or idle chatting, sending mass mailings or chain letters.
- Should assume that any software they did not create is copyrighted. They may neither distribute copyrighted or proprietary material without the written consent of the copyright holder nor violate copyright or patent laws concerning computer software, documentation, or other tangible assets.

- Shall not use the College computer systems to violate any college policies, or rules in the Employee Handbook, Faculty and Student Handbooks or any local, state or federal laws.
- Should disclose to the appropriate authorities (OIT, Security) misuses of computing resources or potential or real vulnerabilities identified in computer systems.

In connection with inquiries into possible abuses, the College reserves the right to examine files, programs, passwords, accounting information, printouts or other computing material without notice.

COMMON FORMS OF COMPUTER ABUSE

Computing resources are valuable, and their abuse can have a far reaching negative impact. Computer abuse affects everyone who uses computing facilities. The same moral and ethical behavior that applies in the non-computing environment applies in the computing environment. In providing computing resources, the College has the responsibility of informing its users (faculty, staff and students) of the rules, regulations and procedures regarding their usage. Computer users are responsible for understanding these rules so that they can abide by them. The College considers the following topics as areas of abuse:

A. PRIVACY

Violations include attempting to access another user's computer files without permission; supplying or attempting to supply false or misleading information or identification in order to access another user's account; deliberate, unauthorized attempts to access or use the College's computers, computer facilities, networks, systems, programs, or data, the unauthorized manipulation of the College's computer systems, programs, or data.

B. THEFT

Theft includes the stealing of any property of the institution, Board of Governors, ATC, or State of West Virginia. Unauthorized use of your funding allocation, or that of another user, whether billable or not, is also considered to be theft.

C. VANDALISM

Attempted or detected alteration of user system software, data or other files, equipment or disruption or destruction of resources, unapproved installation of software applications or operating systems is considered vandalism.

Violation includes, but is not limited to:

1) sending programs or files which will replicate themselves or damage user accounts;
2) tampering with or obstructing the operation of the College's computer systems (attempting to "crash" the system);
3) distributing or attempting to distribute data or software without proper authorization;
4) attempting to or interfering with the performance of a College computer; or
5) damaging computer hardware or software.

D. COPYRIGHT ISSUES

WVNET and the College have purchased licenses to a number of proprietary programs. Distribution of software shall be documented by the College OIT and centrally managed. Therefore, the redistribution of any software from the College computing systems, without authorization from the College OIT, is strictly prohibited. Public domain, or "open" licensed software may be installed with proper notification of the College OIT.

Copyright violations include, but are not limited to, copying, transmitting, or installing data, software or documentation without proper authorization or attempting to do so.

Internet Piracy includes using the Internet to infringe on copyrighted works. Using any computer connected to the College's network (Ethernet/Wi-Fi/VPN) to obtain copyrighted works illegally via the Internet may result in loss of computer privileges, academic suspension, or other punishments dictated by law.

E. HARASSMENT

Harassment of other users can include the sending of unwanted messages or files. This includes, but is not limited to, the use of email, chat, social media, and message boards.

Violation includes, but is not limited to, interfering with the legitimate work of another user; the sending of abusive or obscene messages via computers or electronic device; the use of computing resources to engage in abuse of other users.

F. CYBERBULLYING

Cyberbullying is defined in legal glossaries as:

1) actions that use information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm another or others.
2) use of communication technologies for the intention of harming another person
3) use of internet service and mobile technologies such as web pages and discussion groups as well as instant messaging or SMS text messaging with the intention of harming another person.

Examples of what constitutes cyberbullying include communications that seek to intimidate, control, manipulate, put down, falsely discredit, or humiliate the recipient. The actions are deliberate, repeated, and hostile behavior intended to harm another. Cyberbullying has been defined by The National Crime Prevention Council: "When the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person."

G. MISCELLANEOUS

Other inappropriate uses include: unauthorized and time consuming recreational game playing, unless in support of recognized student clubs or authorized activities; using computer accounts for work not authorized for that account; sending chain letters or unauthorized mass mailings; using the computer for personal profit or other illegal purposes; personal advertisements.

DISCIPLINARY ACTION FOR ABUSE OF POLICY

The College takes seriously any breach of policy. Abuse or misuse of College computing services may not only be a violation of College policy and user responsibility, but may also violate state and federal criminal code. Therefore, the College will take appropriate action in response to user abuse or misuse of computing services. The College will take appropriate steps to identify the offending party and suppress the activity. Action may include but is not necessarily limited to: revocation of student, faculty, or staff computing privileges; suspension for students; suspension or termination of employment; or other legal action including recovery of damages and/or referral to law enforcement authorities.

Finally, the College promotes the use of its computing facilities and seeks to improve the computer literacy of its users. Reducing computer abuse provides more computing resources for users with legitimate computing needs. Every user is expected to comply with this policy.

DEFINITIONS

Authorized User - Authorized Users are to have valid accounts issued by the Office of Information Technology ("OIT"). These account usernames and passwords are not to be shared. Authorized Users will be held responsible for any misuse of their account, including use of their account by non-authorized users.

Copyright Laws - the College requires that only licensed software be installed on college computing resources. Authorized Users are required to request permission before installing software, and permission will only be granted after all licensing requirements have been met.

Game Playing - Recreational game playing is prohibited.

Hacking - Attempting to possess or possessing other user's passwords, attempting to disrupt or disrupting computer systems, or unauthorized access of is considered hacking and is prohibited.

Harassment - Sending unwanted messages, abusive or obscene messages, chain letters, mass mailings, or intruding on a user's account is considered harassment and is prohibited.

Individual Privileges - An Authorized User is granted the privilege to use computing resources for productive purposes, and his/her privileges are contingent upon acceptance of accompanying responsibilities.

Miscellaneous - Using accounts for mass mailings, personal profit, or illegal purposes is prohibited.

Approved by: Cabinet **Date:** 4/1/2014