BLUEFIELD STATE COLLEGE
BOARD OF GOVERNORS
POLICY NO. 54

TITLE: INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

SECTION 1. GENERAL INFORMATION

1.1 Scope: This policy set standards of acceptable use of the information technology environment at Bluefield State College. It includes, but is not limited to, electronic mail, pornography, wireless, social media, and mobile devices. This policy applies to all people using Bluefield State College's Information Technology Environment (ITE), including staff, faculty, students, contractors, visitors and affiliates.

1.2 Authority: W. Va. Code §18B-1-6

1.3 Replaces Policy D.1400

1.4 Filing Date: May 29, 2014

1.5 Effective Date: April 9, 2014

1.6 Control over: All Bluefield State College Information Technology Resources

SECTION 2. POLICY

2.1 Introduction**:** Information technology is playing an increasingly important role in the life of each individual, and consequently to the Bluefield State College community. Access to these finite resources is a privilege and is provided with an expectation of responsible and acceptable use. In addition to the principles and guidelines provided in this policy, institutional policies along with certain federal, state and local regulations apply to the use of the Information Technology Environment (ITE).

2.2 General Principles and Guidelines: The basic premise of this policy is that responsible and acceptable use of the Bluefield State College ITE does not extend to whatever an individual is capable of doing. Instead, certain principles provide a guide to users regarding responsible and acceptable behaviors and users are responsible for knowing and understanding them. These principles and guidelines include, but are not limited to:

2.2.1 The Bluefield State College ITE was funded and developed for the sole purpose of promoting and supporting the mission of the College.

2.2.2 Authorized users of the Bluefield State College ITE, or College sponsored resources such as WVNET are those individuals who have been granted a username and password. The username and password combination are the user's identity and license to

access and use the components of the Bluefield State College information technology environment for which users are specifically authorized.

2.2.3 Authorized users will abide by institutional policies along with applicable local, state and federal regulations.

2.2.4 The resources of the Bluefield State College ITE are finite and shared. Appropriate and responsible use of these resources must be consistent with the common good. The ITE may NOT be used for commercial or profit-making purposes.

2.2.5 The College reserves the right to limit access to the Bluefield State College ITE when investigating cases of suspected abuse or when violations have occurred.

2.2.6 Use of the ITE is a privilege and not a public forum, therefore the College reserves the right to restrict or deny usage of the ITE when such usage does not promote or support the mission of the College.

2.2.7 Users must adhere to the ethical standards governing copyright, software licensing, intellectual property, and proper downloading of data (i.e. Music, Video,…).

2.2.8 Personal web pages may NOT contain the official Bluefield State College logo.

SECTION 3. ELECTRONIC MAIL (EMAIL)

3.1 This policy establishes the applicability of law and other Bluefield State College policies relating to electronic mail. The College recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. The College affords electronic mail privacy protections comparable to that which it traditionally affords paper mail and telephone communications.
The College encourages the use of electronic mail and respects the privacy of users. It does not routinely inspect, monitor, or disclose electronic mail without the holder's consent. Nonetheless, subject to the requirements for authorization, notification, and other conditions specified in this policy, the College may deny access to its electronic mail services and may inspect, monitor, or disclose electronic mail when required by and consistent with the law. The College will not attempt to regulate the content of a person's electronic mail and accepts no responsibility for the content of electronic mail.
Although it is impossible to ensure the confidentiality of any electronic message stored or communicated through the computing facilities, this policy articulates the procedures adopted to provide users with a secure mail environment. Electronic mail is a privileged communication between the parties involved and will be subjected to the same protection afforded traditional paper mail. The purpose of this section is to describe (1) Qualifications for Email, (2) Postmaster Responsibilities, (3) Undelivered Email, (4) Email Violations, (5) Discovery of Illegal Activity, (6) File Backup, (7) Email Maintenance, and (8) Email Violations Procedure.

3.1.1 Qualification for Email: All Bluefield State College faculty, staff, students, and alumni qualify to receive an email account. Email accounts will be automatically created for any person who is an entering student or for any faculty or staff personnel upon employment. As of August 19, 2013, all Bluefield State College business related communications among students, staff, and faculty members will be conducted via the official Bluefield State College email system. Students must utilize the official Bluefield State College email account that is assigned upon admission to the institution. Staff and faculty members must utilize the official Bluefield State College email account that is furnished upon initial employment. Other Email domains such as @hotmail.com, @yahoo.com, @msn.com, @gmail.com, etc. will not be recognized as official communication from Bluefield State College. Information about these accounts is attainable through the College Computing Services department in Suite 123 of Dickason Hall.

3.1.2 Postmaster Responsibilities: The postmaster is the person assigned responsibility for dealing with email related issues at Bluefield State College. It may be necessary at times for the postmaster to read an electronic mail header which has failed to reach its destination to determine, if possible, the intended addressee and redirect the message to the correct address. However, it is not the practice of the postmaster to read or to discuss the content of any message. The postmaster is a staff member of the Bluefield State College technology area and is assigned by the Director of Computer Services. The postmaster will read the mail only to the extent necessary to assist in proper mail delivery. Copies of the messages will not be retained after successful redirection, nor will the postmaster discuss the contents of the messages with others.

3.1.3 Undeliverable Email: The computer system automatically forwards all undeliverable mail to the designated postmaster and/or returns it to the sender. This is a standard feature of many mail systems. Typically, the postmaster checks the address and, where appropriate, re-sends the message to the correct address. In general, incorrectly addressed outgoing mail is ignored, while incoming email is redirected to its intended recipient.

3.1.4 Email Violations: In general, policies and restrictions outlined in state (Electronic Mail Protection Act, West Virginia Statute, House Bill 2627) and federal laws and the Faculty, Classified Staff or Student Handbooks are applicable when using electronic mail. Specific examples include, but are not limited to the following:

- Forged Mail- It is a violation of this policy to forge an electronic mail signature or to make it appear as though it originated from a different person.
- Intimidation- It is a violation of this policy to send electronic mail that is abusive or threatens an individual's safety. The use of electronic mail for sexual, ethnic, religious, or other minority harassment is also prohibited. Known threats to personal safety will be reported to Campus Police.
- Harassment- It is a violation of this policy to use electronic mail to harass an individual. This includes sending or forwarding chain letters, deliberately flooding a user's mailbox with automatically generated mail, inappropriate email

messages, and sending mail that is deliberately designed to interfere with proper mail delivery or access.

- Unauthorized Access- It is a violation of this policy to attempt to gain access to another person's mail files regardless of whether the access was successful or whether or not the messages accessed involved personal information.
- Illegal Use of Mail Services- It is not only a violation of this policy to send copyrighted materials electronically - it is a federal offense. All violations will be dealt with accordingly and/or reported to the proper authorities.
- Chain Letters/Junk Email – It is a violation of College policy to send chain letters and junk email. A chain letter is a letter sent originally through national and international mail services and now through networks such as the Internet. The original intent was for young people, mostly students, to meet peers of the world. Writers shared such things as their community environment, their schools, their friends, and many times about their family life. Junk email is email sent as commercial transactions, personal business, and other non-College activities. The negative side to chain letters and junk email on the Internet, or any other network, is that it fills the net and the mail servers with useless junk at the expense of the subscribers who use the Internet mail legitimately.
- Spam– It is a violation of College policy for anyone to "Spam" from College mail servers. Spam is exploiting servers or similar broadcast systems for purposes beyond their intended scope.
- Hoaxes– It is a violation of College policy to distribute an email hoax with the intention to mislead or trick others into believing or accepting or doing something, so as to bring about the belief in or acceptance of what is actually false.
- Attachments – Attachments are any items added in addition to the original email being created. Attachments must adhere to the section on illegal use of the mail services above. Attachments have a direct effect on all mail servers and recipients, so an attachment should not exceed 10 MB. Large attachments should never be sent in mass mailing.

3.1.5 Discovery of Illegal Activity: Any messages whose content is clearly illegal should be reported to the "Computing Services Help Desk", appropriate campus official(s) or to the Campus Police Office. Such items might be discovered as part of normal Postmaster activity, dead letter processing, contact from local/state/government agencies or other tasks. Examples might include messages containing illegally obtained credit card numbers, telephone authorization codes, grade reports, criminal conspiracy, illegal transmission of copyrighted materials, or similar items. Users will be held accountable for all actions performed with their email account, including those actions performed by other individuals as a result of user negligence.

3.1.6 File Backup: Mail files are copied as a routine aspect of system backups. This is an automatic process that does not involve any human reading of the files copied. Such practices are not considered a violation of privacy.

3.1.7 Email Maintenance: Accumulating old email is similar to saving a person's old letters in order to re-read them in the future. Storage of electronic email requires disk storage on a server or the user's computer. The user controls storing email on their computer, but email stored on the College server is subject to the Email Postmaster, and the Postmaster retains the right to delete items from any mailbox and/or the trash folder that are older than 6 months.

3.1.8 Email Violations Procedure: The College reserves the right to authorize disconnecting a user's account if the user represents a threat to system or mail integrity. As part of an investigation, the College may examine mail files, logs, and any other appropriate documents or testimony. The appropriate Faculty, Staff or Student Handbook, local, state or federal law, shall determine any necessary disciplinary action.

SECTION 4. PORNOGRAPHY

4.1 The College aims to prevent its staff, students, visitors and contractors from having unnecessary contact with pornographic material accessed through the Information Technology Environment (ITE). Contact with such material may not only be offensive but could also be construed as a form of harassment. All types of harassment are unacceptable, discriminatory and, in certain circumstances, unlawful. This Code aims, in particular, to prevent and address harassment arising from the use of College ITE facilities, or ITE facilities used on College premises, to access, display, generate, distribute, forward or store pornographic material. The College seeks to maximize the opportunities afforded by ITE for teaching, research, and administration; however these facilities must be used acceptably, responsibly, and legally. In particular, using ITE facilities to access, display, generate, distribute, forward or store material which may be offensive, pornographic, obscene or abusive is unacceptable and, in many cases, illegal. All such incidents will be treated seriously and could provide grounds for disciplinary action leading to dismissal or expulsion from the College. The College takes breaches of this Code seriously and will co-operate with efforts to prosecute anyone using its ITE facilities unlawfully. If College ITE facilities are used in connection with pornographic material, a complaint should be made to the Director of Computer Services, the Director of Instructional Technologies, the Director of Human Resources, or the head of department/division who will decide if the matter should be reported to Campus Police Office or if it can be dealt with by the College procedures outlined below.

4.1.1 Reasons for this Policy: Using ITE facilities in connection with pornographic material is unacceptable to the College and may also be contrary to federal or state law. Furthermore, using ITE facilities in connection with pornographic material also contravenes the College's Policy on Harassment. Harassment has legal implications in various types of legislation, including Health and Safety law. If such activities are not discouraged the College's internet link could be suspended and this would have far reaching negative implications.

4.1.2 Definitions: ITE pornography is understood by the College to be material of an explicit sexual nature which is made available, displayed, generated, distributed,

forwarded or stored using ITE facilities such as the internet, software packages, email, storage devices, mobile devices or computer hardware. The pornographic material may be in the form of visual texts, including photographs or moving images, such as video files including mpg, avi, and ram files, or written texts and may depict, for example, bestiality, pedophilia, sexual torture, incest, lewd display of genitalia, or depictions of lewd sexual activity. The College acknowledges two exceptions to the Code outlined here. Firstly, the College is mindful that there is legitimate study and research into ITE pornography and associated issues and this is the only reason for deliberately accessing such material. Individuals must be able to show that the access is necessary to their work or studies and they are expected to exercise discretion to ensure that the spirit of the College's Comprehensive Information Technology Policy is not contravened. They should take great care also that the material is not stored or displayed in a way that would offend others who may come into contact with it. Secondly, there may be incidents involving the unsolicited receipt of ITE pornography and the College would NOT discipline an individual in such circumstances.

4.1.3 ITE Pornography Complaints Procedure: Action may be taken at two levels to address complaints of ITE pornography and these are outlined below. In less serious cases, it may be sufficient that disciplinary action is taken by the appropriate College authorities, such as systems managers. Other cases will be referred to Campus Police. A member of the Campus Police will decide on the severity of the offence. In general, the College will hand to the police incidents in which there is: pornographic material involving moving images; pornographic text or images with personal reference to the recipient; pornographic material circulated from Bluefield State College to other organizations; pornographic material of a pedophile nature or containing references to bestiality. Advice on dealing with complaints about ITE pornography can also be obtained from the Director of Computer Services, Director of Instructional Technology Center, Director of Human Resources, or the Director of Campus Police.

4.1.4 Faculty/Staff: Any member of the faculty or staff found to have transgressed this policy with regard to ITE pornography will be subject to disciplinary action in accordance with their conditions of service. Disciplinary action may take the form of a verbal or written warning and, for serious misconduct, demotion, transfer or dismissal. Incidents of a more serious nature will also be referred to the Campus Police and the College authorities will be informed.

4.1.5 Students:Any student found to have transgressed this Policy with regard to ITE pornography will be subject to disciplinary action as outlined in the Student Handbook.

4.1.6 Monitoring: Incidents of ITE pornography dealt with by the College including those referred to the Campus Police will be tracked on an annual basis by Computing Services.

4.1.7 Responsibilities: The cooperation of all College staff, students, contractors and visitors is essential to ensure the success of this policy. The College is committed to acting positively to prevent and address incidents involving pornography and is involved

in programs of staff training to heighten awareness about this important matter as needed.

SECTION 5. WIRELESS LOCAL AREA NETWORKS (WLAN) OR WIFI

5.1 This policy is required to protect Bluefield State College's network infrastructure from uncontrolled or unauthorized access that could result in intellectual property loss or data destruction and to provide a consistent interface and procedure for use by the Bluefield State community. Wireless Local Area Networks (WLAN) or WiFi networks are by nature an open transport technology that can be inherently insecure and therefore any extension to the College's networks using this infrastructure must be authorized by Computer Services prior to procurement and implementation.

5.1.1 General Principles and Guidelines: Security and access control will be implemented and any visitor to Bluefield State College requiring wireless access may be required to register with Computer Services prior to date needed allowing 24 hours for the request to be processed. Computer Services will work to maintain internet access as open as possible consistent with security requirements. Radio propagation and channel management will be controlled by Computer Services to prevent interference and unintentional spill. All wireless access nodes added must be approved and configured by Computer Services to ensure appropriate security is enabled and correct operation with existing equipment. No wireless device can be used to provide private network services for downstream unregistered user equipment or services. Commercial propagation of WiFi services onto the College's sites needs to be formally registered and pre-approved by Computer Services. Computer Services will monitor the network for rogue wireless implementations and has the authority to disable and disconnect immediately upon detection. Any breach of this policy may result in network privileges being revoked. Computer Services will work with departments to accommodate special needs, where technically feasible and cost justifiable. Computer Services will collaborate with academic departments where devices used for specific educational or research applications may require specific solutions. Wireless networking has the potential to make it very easy to gain unauthorized access to the College network based resources. However, the Privacy Act 1993 places an onus on organizations to protect information from inappropriate access by unauthorized parties. There is a significant amount of information held on the College's network and it is therefore important to ensure that only authorized people have access to this resource.

SECTION 6. ELECTRONIC SURVEYS

6.1 Surveys and inquiries which are addressed to Bluefield State College faculty, staff, and/or students must be approved and administered by an official unit of the College. The survey instrument may also require approval by the Office of Institutional Research and Effectiveness. Surveys conducted on or off campus in the name of the College by an official unit of the College should be relevant to the surveyed constituency. Procedures and survey request and requirements document can be found on the Institutional Research and Effectiveness website.

SECTION 7. COMMENTARY: INTRODUCTION AND ANALOGIES

7.1 The Information Technology Environment discussed above consists, not only, of the superficial wires, equipment and devices of the data, voice, video, and more conventional information networks on our campuses (and the world) but also the more subtle milieu created by the integration of these technologies into our everyday life situations. In this respect the whole is much greater than the sum of the parts and thus the effect of inappropriate use of this resource can be much greater than might be imagined. This should not be a cause for hesitation about its use but merely a call for thoughtful consideration of action.

In describing the responsibilities and acceptable behaviors related to the Information Technology Environment, certain analogies can be drawn. Social norms, behaviors, and responsibilities associated with the use of electronic communication, publication, media, and access authorization are no different than the conventional mediums with which we are all familiar, i.e.:

- Email or electronic mail is just another form of mail or communications,
- Posting to a news group is the same as posting a notice or comment on a bulletin board, newsletter, letter to the editor, call to a talk show, etc.,
- Participating in a chat group is the same as participating in discussions anywhere a group might congregate face-to-face e.g. in a class, the student center, recreation room, lounge, church group, etc.,
- Creating a WWW or World Wide Web presence is publishing (i.e., making public) a person's own magazine, memoirs, diary, biography, press release, newsletter etc. Consequently, the person is not only, typically, the author but also, perhaps more importantly, the person becomes the editor and publisher and is responsible for their publication from a legal standpoint. Even though Bluefield State College is not the publisher, editor, or author it is the provider of the resource and, as such, is associated with the publication. Therefore, Bluefield State College maintains the right to restrict or deny use of this resource when usage does not promote or support the mission of the College or the State of West Virginia.
- User ID and password combinations are a person's identity and license to use and access limited portions of the ITE. In this sense they are like the person's BSC identification card or a driver's license. Impersonating another individual or allowing impersonation by another individual is not acceptable behavior.
- The computing systems used for mail, WWW, and other technologically augmented services are similar to an assigned work or office space. The space (and some of the content) belongs to Bluefield State College and the State of West Virginia but other personal items may exist in the room. In this sense BSC has an obligation to provide a reasonable amount of security to protect a person's personal property but cannot assume full responsibility for it nor guarantee full privacy.

Similarly, as in a person's work or office space, in the course of normal maintenance of the ITE, certain information may be seen by those attending to the maintenance. All employees of Information Technology are instructed that the disclosure of this information is a punishable offense (as is the willful intrusion without cause). Also, in a similar manner, a person is allowed the use of certain space and accouterments and is

expected to utilize them in a responsible manner by taking proper care, providing reasonable security, and respecting the property and privacy rights of others occupying similar spaces and their assigned, and private resources.

SECTION 8. COMMON FORMS OF VIOLATIONS

8.1 Although most users strive for acceptable and responsible use of the ITE, inexperienced users may unwittingly engage in behaviors that violate the principles and guidelines of responsible and acceptable use. To that end, this section outlines some of the more common forms of violations that occur. These examples should not be interpreted as an exhaustive list of violations. Questions regarding the appropriateness of specific behaviors should be directed to Computing Services.

- Furnishing false or misleading information or identification in order to access another user's account
- Using another person's username/password or permitting someone else to use your username/password
- Investigating, reading or attempting to access another user's files without permission
- Attempts to access or manipulate certain components of the information technology environment without authorization
- Alteration of software, data, or other files without authorization
- Disruption or destruction of equipment or resources
- Using subterfuge to avoid being charged for computer resources or deliberate, unauthorized use of another user's account to avoid being billed for services
- Copying or attempting to copy data or software without authorization
- Interfering with legitimate work of another user
- Sending abusive, harassing, or obscene messages
- Viewing or listening to objectionable, obscene, pornographic, or harassing material in public areas
- Excessive recreational use of resources
- Any activity or action that violates the University's Student Code of Conduct or Policies, faculty/staff policies and regulations, or federal, state, or local laws.

SECTION 9. ENFORCEMENT

9.1 Violation of these guidelines constitutes unacceptable use of information resources, and may violate other College policies and/or state and federal law. Suspected or known violations should be reported to the appropriate ITE computing unit. The appropriate College authorities and/or law enforcement agencies will process violations. Violations may result in revocation of computing resource privileges, academic dishonesty proceedings, faculty, staff or student disciplinary action, or legal action.
The maintenance, operation, and security of computing resources require responsible College personnel to monitor and access the system. To the extent possible in the electronic environment and in a public setting, a user's privacy will be preserved. Nevertheless, that privacy is subject to the West Virginia Access to Public Records Act, other applicable state and federal laws, and the needs of the College to meet its administrative, business, and legal obligations.

The office of Computer Services is authorized to engage in investigations and apply certain penalties to enforce this policy. These penalties include, but are not limited to, temporary or permanent reduction or elimination of access privileges to any or all of the components of the ITE. If, in the opinion of Computing Services, it is necessary to preserve the integrity of facilities, services, or data, Computing Services may suspend any access, whether or not the account owner is suspected of a violation. In such a case, Computing Services will attempt to notify the user of any such action after the potential threat to the facilities, services, or data is contained. If such an investigation is required it will be done only under the direct authorization of the Director of Computing Services and all effort will be made not to disclose any content to anyone other than those with a need to know during the investigation or adjudication of the alleged offense. Consequences of the discovery and investigation process or normal maintenance might include the inspection of files contained in an individual's storage space or monitoring selected traffic on the networks. Again, all effort will be made not to disclose any content to anyone other than those with a need to know. However, where there are moral, ethical, or legal implications of the nondisclosure of such information Computing Services personnel are similarly instructed to contact the Director of Computing Services, who, may authorize its disclosure to appropriate authorities if deemed warranted. In most cases an individual accused of a violation of this policy will be notified and have an opportunity to respond before a final determination of a penalty is made. The Director of Computing Services or their designee, in conjunction with other responsible parties (e.g., College Council, Student Judicial Affairs, Academic Affairs, or Human Resources) will examine the available evidence and circumstances. If a penalty is levied, the decision may be appealed through the appropriate channels.

SECTION 10. GENERAL INFORMATION AND DEFINITIONS

10.1 Access Nodes: This is the device that is connected to the wired network and provides wireless access for devices to resources on the network.

10.2 Channel: A channel is a communications path based on different frequencies that access points and devices can select to communicate.

10.3 Protocol: This is the communications language used between peers.

10.4 Radio propagation: This is the transmission and reception area covered by the access point where access to service can be achieved.

10.5 Wireless devices: This is an assortment of electronic devices and could include but is not limited to a computer, tablet, personal digital assistant (PDA), laptop, or mobile device.

10.6 WLAN: Local area networks that use wireless communication defined by the IEEE 802.11 standard.

If any provision of this policy is ruled invalid under law, it shall be deemed modified or omitted to the extent necessary, and the remainder of the policy shall continue in full force and effect.

Adapted with permission from Massey College Policy Guide and Marshall University Acceptable Use Policy and Wireless Communications and Networking Procedure.