West Virginia School of Osteopathic Medicine

INSTITUTIONAL POLICY: GA-31

CATEGORY: General Administration
SUBJECT: Acceptable Use of Information Technology Resources
EFFECTIVE DATE: November 9, 2010
LAST REVISION DATE: N/A
APPLICABILITY : Faculty, Staff, and Students

GA 31-1. Authority

1.1 WV Code §18B-1-6

1.2 WV CSR §133-4

GA 31-2. Purpose

This Acceptable Use Policy for information technology (IT) resources at WVSOM is to provide, promote, and establish the secure, ethical, and legal use of data, devices, and electronic communications for all constituents of the institution. This includes staff, faculty, students, alumni, State Wide Campus entities, and guests. It is governed by institutional policies as well as local, state, and federal laws relating to security, copyrights, and other statutes regarding electronic media. All faculty, staff, and students should have completed the Acceptable IT Usage Course in the SOLE Course Management System before utilizing their WVSOM account for network and email access.

GA 31-3. Definitions

3.1 Firewall. A combination of hardware and software used to prevent unauthorized access to networks when certain security criteria are not met.

3.2 Gateways. Entrance into a network.

3.3 In the cloud. Shared computer resources outside of WVSOM's internal network accessed securely via the internet for virtual applications such as email.

3.4 Network. A group of interconnected computers, computer peripherals, and other technology resources which is constructed in a particular topology for electronic access and communication to other technology resources based on certain protocols and rules.

3.5 Network authentication. The process of confirming an allowable identity onto a network with a user ID and password as "credentials" for entry.

3.6 Network authorization. The verification that an authenticated identity is allowed to access certain technology resources and network areas *after* it has been allowed entry to the network.

3.7 Packet shaping. Controlling network traffic in order to eliminate bottlenecks or over consumption of resources.

3.8 Polling. A process which is repeated and continuously trying to gather data that can compromise network operations.

3.9 Server. A larger capacity computer which is being used for a specific purpose such as print, email, web or file services, or the hosting of specific applications such as Student Information Systems.

3.10 Spoofing. A technique used in hacking to gain unauthorized access to a restricted technology resource by pretending to be a trusted source.

3.11 Sync. The process of sharing data, specifically passwords, to another WVSOM application (i.e. email) to avoid maintaining multiple passwords.

GA 31-4. Shared Resources

4.1 The WVSOM academic atmosphere encourages the sharing of knowledge and the collaboration that should occur in the educational and research environment. The Information Technology Department has part of its mission "the enhancement of the delivery of medical education through the latest technology initiatives." In support of this mission, to maintain the highest standard, most innovative and quality based technologies, adherence to acceptable usage is critical. Access to systems and networks, owned or operated by WVSOM, carries certain responsibilities and obligations and is considered a privilege. When utilizing information technology systems, users should value the physical facilities, the integrity of the information resources, and all license and contractual agreements related to the resources.

4.2 Due to the shared nature of IT resources, users should:

4.2.1 Be considerate of others and refrain from monopolizing systems;

4.2.2 Avoid overloading networks with excessive data, degrading services, wasting computer time, as well as connection time, disk space, printers, and other peripherals associated with IT;

4.2.3 Only use resources for authorized purposes;

4.2.4 Protect user IDs and passwords from unauthorized use;

4.2.5 Use only IT resources which you are authorized by WVSOM to access;

4.2.6 Only use legal versions of copyrighted software in compliance with vendor license requirements; and

4.2.7 Report unauthorized use, damaged systems, and malfunctioning software to the Information Technology Department.

4.3 Users should refrain from non-mission critical unapproved activities and the activation of unauthorized devices, which may compromise and/or consume network bandwidth or disrupt other institutional services.

GA 31-5. Ownership of Information Technology Resources

5.1 As an academic institution, WVSOM utilizes technology in many aspects of this environment: computer systems, printing devices, telephones & voice mail, electronic

mail, internet & web services, databases, video conferencing, course management, training events and networking. Departments may have specific software applications and systems for functions inherent to their area of expertise. As such, departments may make additional requests of users above and beyond this Acceptable Use Policy

5.2 In addition to campus-wide service agreements for specific software vendor licenses purchased by the IT Department, other departments may request purchase of specially licensed software. Licenses are normally purchased by the number of intended users. Therefore, it is a violation of software license agreements to make copies of software without permission. Users should abide by the software license agreements and NEVER make copies of software someone else has purchased and owns.

5.3 WVSOM owns computers in the library, training labs, State-Wide Campus sites, departments, and at employee work stations, along with the campus network, servers, switches, routers, cabling, and attached peripherals such as printers. WVSOM determines who has access to these information technology resources and is providing this Acceptable Use Policy that governs their usage. Overuse of these resources can result in denial of access or a reduction of use for the benefit of other users and mission critical applications.

GA 31-6. Data Protection

6.1 Regulations

6.1.1 As an academic institution with the mission of educating future Doctors of Osteopathic Medicine, WVSOM is governed by:

6.1.1.1 The Federal Educational Rights and Privacy Act (FERPA) http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

6.1.1.2 The Health Insurance Portability and Accountability Act (HIPAA) http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

6.1.1.3 The Gramm-Leach-Bliley Act http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

6.1.2 FERPA requires that WVSOM protect each student's educational records including placement, medical, financial, disciplinary, and academic information. WVSOM cannot disclose this information without the written consent of the individual student. Parents and guardians do not have extended access to these records. Directories, lists, and addresses cannot be released to non-affiliated WVSOM entities if the student has requested confidentiality. A student's personally identifiable information cannot be posted publically without written consent by the student.

6.1.3 HIPAA requires:

6.1.3.1 That health information be protected and safeguarded against unauthorized use. It contains two sub-components for privacy issues: the Privacy Rule and the Security Rule. The intent of the Privacy Rule is to protect the patient's right to privacy, but allow adequate flow of information for health services to be provided. Protected health information cannot be disclosed or used without written authorization by the individual whose data is to be

accessed. The Security Rule specifically addresses the protection of information in electronic format, both in technical and non-technical terms surrounding health provider operations. The electronic data must adhere to administrative, physical, and technical standards set forth by the Security Rule.

6.1.3.2 Any breach of information relating to HIPPA must be reported in accordance with the Health Information Technology for Economic and Clinical Health Act (HITECH Act), requiring notification to covered entities and their associations.

6.1.4 The Gramm-Leach-Bliley Act regulates the privacy surrounding personally identifiable financial information, including credit card and bank account numbers.

6.1.5 Because of the sensitive nature of student, employee, patient, and donor information at WVSOM, extreme care and precautions should be taken in the storage and retrieval of the data. Only data that you are authorized to view should be accessed.

6.2 Passwords

6.2.1 The key to protection of this data is the proper utilization of usernames, accounts, and passwords. Passwords should not be "guessable" and should be changed frequently. When creating passwords the following rules should be applied:

6.2.1.1 Passwords must be at least nine characters in length;

6.2.1.2 Passwords may not contain the user name or any part of the user's full name; and

6.2.1.3 Passwords must contain at least one upper case letter, one lower case letter, and one number. For example, Ghrabc469 is a valid password.

6.2.2 Passwords should be committed to memory and should never be stored in close proximity or easy access to your computer system. If your system is left unattended, you should log out of applications and your account, or create a password protected screen saver.

6.3 Storage and Destruction

6.3.1 Electronic media, such as CDs, that are no longer used should be destroyed. Media that is still in use should be kept in a fire-resistant, locked cabinet. Before the Information Technology Department surpluses old equipment, hard drives are removed and drilled for security, or using a bootable media disk blank data is written to the hard drive. The department also maintains nightly backups of servers and file shares used by the institution. Any user information that is not backed up by the IT Department should be backed up to electronic media by the user. For students, backups are solely their responsibility. If a user is unsure of the proper backup procedures to follow, they should contact the IT Department for assistance.

6.3.2 Security measures should be extended to laptops, flash drives, and other devices which can contain sensitive data that may not be on-site in a secured office. It is the user's responsibility to guarantee that paper and electronic data is protected against unauthorized use, both on-site and off-site of the Lewisburg campus. This includes electronic files, emails, and all other records relating to students, employees, patients, alumni, and donors.

GA 31-7. Email

7.1 WVSOM's email services are handled in the cloud by the Microsoft Live.edu platform at www.outlook.com. The email services require logging on via an Internet browser or a local setup to the Outlook application to download messages to the PC. WVSOM no longer maintains email servers locally and has entered into a Terms of Use agreement with Microsoft regarding email services. For explicit definitions of this agreement please visit http://domains.live.com/Addendums/enus/EduWithOutlookLive.htm for more information. User accounts may be suspended or discontinued based on violations of Microsoft's Terms of Use Section 2.a.iii. or WVSOM's Institutional Policy GA-32 Email (http://www.wvsom.edu/_pdf/allpolicies/GA32.pdf).

7.2 Each user account will allow 10 gigabytes of email storage. User network and email accounts are assigned for incoming students once the second confirmation deposit is made to WVSOM. User accounts for employees are created once the hire notification has been sent by the Human Resources Department. The accounts are created and passwords will sync from an Active Directory database to the user's email account. Users should never need to change the passwords from within the Outlook application. Passwords should only be changed via the IT link at https://my.wvsom.edu/Scripts/dompass.exe . All official WVSOM email will be sent to the Outlook account to which the user has been assigned. Users do have the option to forward mail from the WVSOM account to any valid email account with another Internet Service Provider (i.e. Hotmail, Yahoo).

7.3 Live.edu does perform spam and phishing filtering. Characteristics of each email message are reviewed at the Outlook gateway to determine legitimacy. An email that has a high rating is deleted, mid-level ratings are sent to the junk mail folder, and valid emails will be placed in the user's inbox. Only specific accounts have been given authority to send out mass emails (Admissions for example). Unless a user has received specific authority from the Information Technology Department, mass emails should not be sent and may be rejected for delivery by Outlook. The Live.edu services have placed a maximum of 100 recipients in any one email. Users should use group lists to avoid this limitation only when necessary.

7.4 Users should understand that there is no right of privacy in email communications or in the monitoring of traffic to accounts. Accounts may be monitored when traffic interferes or presents breakdowns for appropriate functions.

7.5 In accordance with this Acceptable Use Policy users should follow these guidelines regarding email and refer to institutional policy GA-32:

7.5.1 Maintain confidentiality regarding user accounts and passwords;

7.5.2 Notify the IT Department if any breach of security has occurred;

7.5.3 Each email session should be ended when complete so that accounts cannot be compromised;

7.5.4 Complaints regarding email must be made in writing, signed, and submitted to the Information Technology Department;

7.5.5 Email is subject to discovery and production in civil litigation;

7.5.6 All email is the sole responsibility of the person which originated the content and not WVSOM;

7.5.7 Users should never use WVSOM email services for non-sanctioned or non-mission related activities. Email should never be sent for commercial or personal gain;

7.5.8 Forwarding of email chain letters is prohibited. Promises of fame, fortune, or donations to specific causes are generally untrue. These activities are a waste of IT resources, a nuisance to recipients, and can offend others;

7.5.9 Email should never be sent to impersonate another individual or entity as the originator. Email identifiers (i.e. headers) should never be manipulated to disguise its origin;

7.5.10 Email content should never be harmful or unlawful, stalk or harass;

7.5.11 Emails should not collect or store personal data about other users;

7.5.12 Email content should not infringe on any patent, trademark, trade secret, copyright, or other proprietary rights of any party;

7.5.13 Do not execute or open attachments that appear questionable. Contact the IT Department if you are unsure about an email and/or its attachment's legitimacy;

7.5.14 Avoid mass emails. Users should use group lists when necessary;

7.5.15 Refrain from any activity that would cause disruption to email services and network connectivity; and

7.5.16 Follow all state, federal, national, and international laws relating to email accounts and services.

GA 31-8. WVSOM Web Site

The WVSOM web site has been established to support the mission of the institution. All material posted on the site is subject to all applicable regulations and requirements and is subject to authorization and review by WVSOM. The Marketing & Communications Department employs a web master who works in collaboration with the Information Technology Department regarding web site content and functionality.

8.1 Rules and Regulations

8.1.1 A content management application is used to manage the WVSOM web site. Access to the application is provided upon request and following training in its use.

8.1.2 Each page or section is the responsibility of the department or individual who manages that page. All pages relating to the Office of Business Affairs are the responsibility of the VP for Finance and Facilities and his/her designees. All pages relating to any academic department or curricular matter are the responsibility of the VP for Academic Affairs/Dean and his/her designees. All pages related to general institutional matters and the Office of the President are the responsibility of the Web Master under the Director of Marketing and Communications. Posting to the web site requires an approval by the responsible administrator or faculty and the Web Master. This is done using the content management application.

8.1.3 The web site is divided into two domains: the public domain will be open to the general viewing public, while the internal domain will be accessible by Active Directory account and password only. Internal pages will be the sole responsibility of the author of the page. New web pages must be developed by the department or individual responsible for creating it. A template will be supplied and the Web Master will assist with the initial development.

8.2 Prohibitions

8.2.1 The Information Technology Department will maintain the server and take care of technical matters.

8.2.2 The Web Master will design and work with departments regarding page content and structure.

8.2.3 Buying or selling of any non-sanctioned goods and services using WVSOM web pages is strictly prohibited.

8.2.4 Profanity, pornography, generally obscene material, or links to any of the former are strictly prohibited.

8.2.5 Use of any graphic, logo, or picture without the express consent of the creator is strictly prohibited.

8.2.6 Links to other related sites are encouraged. However, wholesale advertising of other organizations and businesses on WVSOM web pages is prohibited.

8.2.7 Any material contained on the WVSOM web site is the sole property of the West Virginia School of Osteopathic Medicine and is subject to the rules and policies contained herein. Any unauthorized use of the site is prohibited.

8.2.8 WVSOM reserves the right to add to or amend the policies governing the WVSOM web site at any time.

8.2.9 The WVSOM server will not be used for personal pages.

GA 31-9. Copyrights

9.1 WVSOM requires that all campus constituents (staff, faculty, students, alumni, State Wide Campus entities, and guests) comply with federal copyright law. Institutional Policy E-40 (http://www.wvsom.edu/_pdf/allpolicies/E40.pdf) specifically addresses this law and guidelines can be found at http://www.wvsom.edu/guidelines/Copyright for further reference. Unauthorized use of copyright protected material may include but is not limited to: software, written word, graphic images, music or audio files, movies, and other digitized material.

9.2 The Digital Millennium Copyright Act process can be utilized to report and respond to any possible violation or infringement of copyright law. WVSOM has registered its designated agent with the U.S. Copyright Office for the DMCA process. In coordination with WVSOM's DMCA agent and the Office of General Counsel, a response to the copyright allegations will be reviewed in accordance with the law. Allegations submitted for review must include:

9.2.1 Digital or physical signature of the exclusive copyright owner or designated licensee or authorized agent of owner;

9.2.2 Description of infringed works;

9.2.3 Description of alleged infringing works;

9.2.4 Complainer's statement that works used is not authorized by law, owner's agent, or owner;

9.2.5 Complainer's statement that notification of alleged infringement is accurate, under penalty of perjury;

9.2.6 Complainer's statement that he/she is authorized by the owner to act regarding one or more exclusive copyright rights; and

9.2.7 Appropriate complainer information that can be used by the DMCA agent for contact.

9.3 After the review, the DMCA agent acting on behalf of WVSOM will seek the appropriate resolution and resolve the matter with the complainer. During the process the web pages that are being reviewed will be taken down until the web master has been instructed regarding the permanent resolution to the complaint.

9.4 WVSOM will assess the effectiveness of compliance to DMCA and the HEOA (Higher Education Opportunity Act) thru annual reviews of:

9.4.1 The process to resolve complaints noted above;

9.4.2 The activities and outcomes generated from the DMCA process; and

9.4.3 Statistical analysis of software/hardware related deterrents used by the Information Technology network infrastructure.

9.5 In addition to the annual review, the IT Department monitors the daily activity of all network login attempts, network authorization, network authentication, and traffic generated to and from local servers hosting various applications and web sites. This includes activities that show abuse of bandwidth, as well as traffic shaping and prioritizing events to the most mission critical to the institution. The WVSOM IT Department has and will institute the most effective methods for capturing violations of DMCA and HEOA, and impose disciplinary action to violators when they are identified. The IT Department currently utilizes packet shaping and firewall technologies for inspecting, classifying, blocking, shaping, and discarding network activities such as illegal Peer-To-Peer (P2P) file downloading. Activities are kept in various web site, application, and database log files for reviewing. Network administrators continually observe and monitor network traffic and possible violations. End users who need legal alternatives for downloading should visit the Educause website for an extensive listing (http://www.educause.edu/legalcontent). The U.S. Department of Education also provides information relating to copyright laws in their annual Federal Student Aid Handbook (www.ifap.ed.gov).

GA 31-10. Network Access

10.1 WVSOM provides both wired and wireless access to the network. Network access is based on the Active Directory user accounts that have been assigned. When accessing the

web site, certain areas are considered public and do not require a log in, other restricted areas will. Those areas that are private will be opened based on appropriate network groups that have been assigned to each user account. A user account may be a member of different groups which will dictate the available network access. Issues with network connectivity can be resolved by contacting the Information Technology Helpdesk at 304-647-6246 or for faculty/staff logging a TrackIt ticket from the web site (https://my.wvsom.edu/TIWeb8/SelfService).

10.2 The following protocols or services are banned from the WVSOM network. A host that is using or offering one of these services will be removed from the network immediately. To learn more about the terms below, please reference a site such as WhatIs or Webopedia:

10.2.1 DHCP Server

10.2.2 RIP (Routing Information Protocol)

10.2.3 IP Routing

10.2.4 IPX Routing

10.2.5 Apple Talk Routing and Apple Talk Protocol

10.2.6 Virtual Hosting via Multiple IP Addresses

10.2.7 SAP (Service Advertising Protocol)

10.2.8 Wireless Access Point

10.2.9 Illegal P2P File Sharing

10.2.10 Multicast Services

10.2.11 Net BEUI Protocol

10.2.12 IPX Protocol

10.2.13 RAS Server (Microsoft Remote Access Server)

10.2.14 WINS Server (The Windows Internet Name Server)

10.2.15 Running an individual NT Domain

10.3 In utilizing the user account for network access to the Internet, good stewardship should prevail. Only internet sites that are needed for institutional mission-related work should be accessed. Users should consider how their activity affects the overall network and guard their accounts from use by other individuals. Users will be held accountable for abusive activity associated with their account including excessive bandwidth from file downloading. Abusive activity will result in the loss of network privileges. The IT Department conducts ongoing audits to collect networking information. This information is used to analyze the state of the network and any abuses that may be occurring. It provides the basis for discontinuing the offending network behavior.

10.4 The Internet is a constant source of unwanted behavior from illegal sources. Certain entities are diligently trying to hack networks, servers, computers, stealing identities, and personal data including usernames/passwords, propagating viruses, phishing, flooding email gateways with spam, and other forms of bad technology related behavior. If you encounter one of these threats or malicious attempts, please report it immediately to the Helpdesk of the Information Technology Department.

GA 31-11. Changing Network User Account Name

11.1 Persons who are given access to WVSOM's network are expected to familiarize themselves with and abide by this Acceptable Use policy. If an individual changes his/her user account, his/her email is also changed. Each student will receive a user account during the School's acceptance and deposit process, while faculty/staff will receive this during the employment orientation. The individual is responsible for maintaining confidentiality of the network user account, and is fully responsible for all activities that occur under the user account.

11.2 The user account can be changed due to marriage, divorce, or other legal name change. The user account must be based on your name and will follow this procedure:

11.2.1 For faculty/staff, requests must be processed through Human Resources, who will verify all legal documentation. For students, requests must be processed through the Registrar, who will verify all legal documentation.

11.2.2 The request is forwarded via e-mail to helpdesk@osteo.wvsom.edu.

11.2.3 The request must include what the account change should be including the last name (i.e. John Smith will be JSmith).

11.2.4 The Helpdesk will notify the individual to review and abide by the Acceptable Use Policy and give an activation date when the change will occur.

11.2.5 If the request is being rescinded, it is the responsibility of the user to notify the Helpdesk prior to the activation date.

11.3 After establishing a new user account, the user will no longer be able to log onto the network or send/receive email using the old account. All subscriptions and mailing lists to the old account must be canceled prior to the account change. New subscriptions and mailing lists must be activated using the new account name after it has become effective.

11.4 When an account is renamed, the new email account will not store the old account messages. Any forwarding that occurred in the old account must be set up in the new account. Additionally, the address book will not contain the old contacts.

11.5 Individual computer profiles contain default configurations such "Favorites." When the name change occurs and the associated profile is changed, all browser settings will be returned to the default. If the user would like to retain this information, it must be backed up before the new account is activated.

GA 31-12. Local Administrative Authority and Installation of Hardware/Software

12.1 Certain computer hardware/software installations require Local Administrative Authority, which is typically reserved for the Information Technology Department. However, specific requests for Local Administrative rights may be reviewed and approved. This requires the user to submit the request form to the Director of Information Technology. If the request is approved, the user assumes all responsibility and actions occurring under the administrative account. The user is prohibited from changing the local administrator password.

12.2 System modifications that are reserved for the IT Department include:

12.2.1 Direct registry additions or modifications by running REGEDIT.EXE or an equivalent utility;

12.2.2 Installation of institutionally approved and licensed software, software upgrades, and service packs;

12.2.3 Installation of all hardware and hardware drivers including printers, scanners, PDAs, speakers, and other peripherals;

12.2.4 Changes to network settings including Internet protocol addressing, destination name servers, gateways, and workstation names;

12.2.5 Installation of any software that has the effect of changing the workstation's basic operating system or changing application components which may degrade network access and throughput; and

12.2.6 Installation and configuration of workstation firewall software.

12.3 Installations that are **strictly prohibited** by the end user include:

12.3.1 Applications that use constant and repeated network and/or Internet polling;

12.3.2 Applications that block or mask workstation identification including applications that create virtual private networks;

12.3.3 Applications that broadcast to random addresses or open addresses;

12.3.4 Software that utilizes network sniffing applications that have the effect of spoofing or masking network identification;

12.3.5 Software that is considered to be spamming or spawning in nature; and

12.3.6 Workstation and local area network management.

GA 31-13. Improper Use

The following list represents a general guideline of activities prohibited while utilizing WVSOM IT resources:

13.1 Use another person's user ID, passwords, and files;

13.2 Use computer programs to decode passwords;

13.3 Access any information without express permission of the owner;

13.4 Attempt to circumvent or subvert system or network security measures;

13.5 Engage in any activity that might purposefully cause harm to systems or to information stored on IT resources, which could create or propagate viruses, disrupt services, damage files, or make unauthorized modifications to WVSOM data;

13.6 Use WVSOM systems for commercial or partisan political purposes, including circulation of advertisements for products or for political candidates via email;

13.7 Make or use illegal copies of copyrighted materials or software, store copies on WVSOM IT resources, or transmit them over the WVSOM network;

13.8 Use mail or messaging services to harass or intimidate another person. For example, broadcasting unsolicited messages, repeatedly sending unwanted mail, or by using someone else's name or user ID;

13.9 Waste information technology resources or network resources, such as intentionally placing a program in an endless loop, printing excessive amounts of paper, sending email chain letters, or sending unsolicited mass mailings;

13.10 Use WVSOM's IT resources or network for personal gain. Selling access to your user ID, access to systems or networks, or performing work with WVSOM assets in a manner not authorized by WVSOM;

13.11 Engage in any activity that would be related to copyright infringement including illegal downloading and P2P file sharing; and

13.12 Engage in any other activity that could compromise WVSOM's IT resources or activities that do not comply with the principles stated in the Acceptable Use Policy.

GA 31-14. Disciplinary Action for Misuse of Information Technology Resources

14.1 WVSOM considers any violation of the Acceptable Use Policy and guidelines to be a serious offense and reserves the right to copy and examine any files or information resident on WVSOM systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations. Violators are subject to disciplinary action as prescribed by institutional policies.

14.2 A student who is found guilty of any of the following acts shall be subject to the maximum sanction of "expulsion" or any lesser sanction authorized by the WV Higher Education Policy Commission and/or the West Virginia School of Osteopathic Medicine Code of Student Rights and Responsibilities (Institutional Policy ST-1):

14.2.1 Disruption or interference with the normal use of computers, computer-related equipment, data, or programs of individuals, the Network, or the WVSOM institution;

14.2.2 Use of equipment, data, or programs in performance of any act listed as prohibited in this Acceptable Use document;

14.2.3 Attempts to breach security in any manner; and

14.2.4 Use of a computer account for other than the purpose for which it is assigned.

14.3 Similarly, staff and faculty will be subject to disciplinary action as a joint effort between the Human Resources and Information Technology Departments. Abuse of any element of this Acceptable Use Policy will result in disabling the user's account, banning the user from access to systems, and possible employment termination. Likewise, alumni and guest accounts may be deactivated based on unauthorized activity.

GA 31-15. Information and Privacy Disclaimer

15.1 Individuals using information technology resources owned by WVSOM do so subject to applicable laws and institutional policies. WVSOM disclaims any responsibility and/or warranties for information and materials residing on non-institutional systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of WVSOM, its faculty, staff, or students. Information on the WVSOM Web site is provided by faculty, staff, students, and organizations. Although WVSOM strives to keep its Web information accurate and up-to-date, accuracy cannot always be guaranteed. WVSOM will not be held responsible for errors or omissions in information provided via the Web site. Visitors to the WVSOM site are responsible for contacting the appropriate person/department to verify information and should not rely on the information contained within the site.

15.2 All activities relating to WVSOM's information technology resources and network may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner by authorized personnel. There is no right of privacy when utilizing WVSOM owned IT resources. Information Technology personnel may give to law enforcement officials any potential evidence of criminal activity found on these IT resources. Use of any WVSOM owned IT resource by any user, authorized or unauthorized, constitutes consent to this monitoring, interception, reading, copying, or capturing and disclosure.