# West Virginia University
# Robert C. Byrd Health Sciences Center

*Student Computer Program*

*Program Information
and
Policies and Procedures
Manual*

*Programs Beginning FY 2014*

# TABLE OF CONTENTS
## *HSC Student Computer Program Policies and Procedures*

### NOTEBOOK HARDWARE/SOFTWARE OWNERSHIP

### POLICIES

## PURPOSE

West Virginia University Health Sciences Center will purchase notebook computers for designated Health Sciences Center students, faculty, and staff. All notebook computers will remain the property of West Virginia University Health Sciences Center until all computer fees are collected from the Student Computer Program participant. Once all computer fees are collected, ownership of the notebook computer will be transferred to the student or HSC department. Students and HSC departments will pay the computer fee over a pre-set number of semesters or via one-time payment option. Check with your school to determine which payment option your school has selected.

## POLICIES

1. All hardware, accessories (modular drives, cables, USB Harddrive(pharmacy, pt/ot only), etc.), software, and software documentation distributed with the notebook computers remain the property of West Virginia University Health Sciences Center during the purchase finance period. Once all computer fees are collected for the notebook, ownership of all hardware and accessories will be transferred to the student or Health Sciences Center department. Ownership of all software and software documentation will be transferred to the student or department at end of purchase finance as long as the software license agreement for the software permits us to do so. Students, faculty, and staff will be notified of what software must be returned.
2. Any student leaving a WVU Health Sciences Center School or Program who has not paid the computer fee in full is required to surrender the issued hardware and software components prior to departure from the School or Program. Students returning the issued hardware and software components will receive tuition reimbursement for the HSC Student Computer Program at the WVU rate.
3. Any HSC employee terminating employment with WVU Health Sciences Center is required to surrender the issued hardware and software components prior to departure.
4. Any student, faculty, or staff in violation of any West Virginia University, West Virginia University Health Sciences Center, and / or HSC Student Computer Program Policies and Procedures shall surrender upon request all hardware and software components to WVU Health Sciences Center Information Technology Services.

**NOTEBOOK HARDWARE/SOFTWARE WARRANTY AND INSURANCE**

**POLICIES**

<u>**PURPOSE**</u>

All notebook computers have extended warranty and insurance coverage – see chart below for the warranty and insurance coverage period for your program.

| Program | Warranty / Insurance Coverage Start Date | Warranty / Insurance Coverage End Date |
|---|---|---|
| Dentistry | July 1, 2013 | June 30, 2017 |
| Medicine | July 1, 2013 | June 30, 2017 |
| Nursing – Aug 2013 start | July 1, 2013 | June 30, 2016 |
| Nursing – Jan 2014 start | January 1, 2014 | December 31, 2016 |
| Occupational Therapy | July 1, 2013 | June 30, 2016 |
| Pathologist's Assistant | January 1, 2014 | December 31, 2016 |
| Pharmacy | July 1, 2013 | June 30, 2017 |
| Physical Therapy | July 1, 2013 | June 30, 2016 |
| Public Health | July 1, 2013 | June 30, 2016 |

<u>**POLICIES**</u>

1. All notebook recipients will be expected to pay for the cost of repairs of any computer equipment that is misused or physically abused.  Notebook components that are broken repeatedly will not be replaced under warranty or insurance and will be the responsibility of the notebook recipient to pay for replacement parts.
2. **There will be a $100.00 per incident deductible for all insurance claims.** Students or HSC Departments, to whom the notebook(s) are issued, will be required to pay the deductible for any insurance claim processed for the notebook – this includes notebooks personally assigned to the student/HSC Department and loaner notebooks assigned to students/HSC Departments.
3. Your notebook has insurance coverage valid in the United States and Canada only.  Coverage includes the notebook only.   Software, case, accessories, personal items, etc. are not covered.  Coverage on the notebook includes theft (requires internal security or police report to substantiate a theft), accidental damage, fire, power surge (UL surge suppression devices must be in use at the time of loss), vandalism, and natural disasters excluding earthquake and flood. Types of losses that are not covered include:  wear and tear, gradual deterioration

or original defects, loss of income, any data or media which cannot be replaced with like kind and quality on the current retail market, mechanical breakdown or faulty construction, damage caused by earth movement, damage caused while being serviced or repaired, loss or damage from fraudulent, dishonest or criminal acts by the owner or user.

4. All notebooks have an extended warranty. Warranty covers malfunctioning hardware such as system boards, memory, DVD, Ethernet, 802.11 wireless.

5. Dentistry and Public Health students: Your ThinkPad notebook battery has a one year warranty. Batteries are considered consumables and are not covered under the extended warranty or insurance after the first year. See the documentation provided with your notebook on how to properly care for your notebook's battery.

6. MD, Nursing, Pharmacy, PT, OT, PA students: Your MacBook Pro battery has extended warranty coverage based on your warranty coverage period. However, please note coverage does not include batteries that have failed or are exhibiting diminished capacity except when the failure or diminished capacity is the result of a manufacturing defect.

7. Pharmacy, PT/OT students: The USB Harddrive has a one year manufacturer's warranty and is not covered under insurance. Students are responsible for replacement and/or repair of these items.

8. Dentistry and Public Health students: Accessories such as the digitizer pen provided with your ThinkPad are not covered under the warranty or insurance program. Students are responsible for replacement and/or repair of these items.

9. The carrying case provided with your notebook has a lifetime warranty. See documentation within the case for detailed information.

10. It is the user's responsibility to provide WVU Health Sciences Center Information Technology Services with the serial numbers of replacement parts as part of a warranty or insurance repair/replacement. This will permit us to update our records and will avoid any confusion for processing future warranty and insurance claims.

# NOTEBOOK SECURITY / THEFT

## <u>POLICY</u>

### <u>PURPOSE</u>

This policy protects West Virginia University Health Sciences Center from fraudulent theft claims.  This policy is applicable to students, faculty, and staff of the Health Sciences Center.

### <u>POLICY</u>

1.  All recipients of Notebook computers shall be responsible for the security of the issued notebook.  Notebooks must be secured at all times.  If there is no internal security or police report to substantiate a theft or if the notebook is left unattended and unsecured, the user will be assessed fair market value for any hardware / software components stolen, or misplaced.  Stolen hardware with a valid security or police report will be replaced through our insurance program.  There is a $100.00 per incident deductible for all insurance claims processed and is payable by the student or HSC Department to whom the notebook computer is assigned - this includes notebooks personally assigned to the student/HSC Department and loaner notebooks assigned to students/HSC Departments.   Lost or stolen software, case, USB drives, personal items, and accessories will not be covered under insurance and will be the responsibility of the notebook recipient to replace.

**APPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES**

<u>**POLICIES**</u>

<u>**PURPOSE**</u>

West Virginia University's computer and information network is a continually growing and changing resource that supports thousands of users and systems. These resources are vital for the fulfillment of the academic, research and business needs of the University community. In order to ensure a reasonable and dependable level of service, it is essential that each individual faculty member, staff member, and student exercise responsible, ethical behavior when using these resources. Misuse by even a few individuals has the potential to disrupt University business, and, even worse, the legitimate academic and research work of faculty and students.

This policy outlines the application of the principles that govern our academic community in the appropriate use of University computer and information network resources. This policy was designed to ensure the proper use of computing resources consistent with the general principles that govern the University. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, individuals' rights to privacy, and freedom from harassment. Computing and networking resources include: computers, computer networks, connections to external computer networks, and subscriptions to external computer services (collectively referred to as information technology or "IT" resources). Open access to these resources is a privilege. It requires individual computer users to act responsibly, conserve computer resources, and consider the rights and privacy of others. Use of any University computing resource constitutes acceptance of this policy.

**Scope**

This policy applies to all University staff, faculty, administrators, officers and students (collectively, "users"), including those on the regional campuses and Extended Learning sites.

**Policy**

West Virginia University IT resources are provided primarily for the use of students, faculty and staff. They are intended to be used for administrative and educational purposes and to carry out legitimate University business. In addition, access to the network may be provided to alumni and members of the local community for the purpose of communicating with students and employees and for accessing University information resources and the internet.

Appropriate use of these resources includes conducting University business, instruction, study assignments, research, communications, and official work of campus organizations and agencies of the University. Access to IT resources is a privilege. It requires individual computer users to act responsibly, conserve computer resources, and consider the rights and privacy of others. The resources have always been, and will remain, the property of West Virginia University. Use of any University computing resource constitutes acceptance of this policy. All users are expected to utilize University resources in a responsible manner consistent with University policies and the guidelines and operating policies that the Associate Provost of Information Technology (CIO) may issue from time to time.

**Prohibited Use of Resources**

Users should be aware that they may be subject to the laws of other states and countries when they engage in electronic communications with persons in such other states or countries or on other systems or networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses. Additionally, users of WVU IT resources must comply with all [federal, West Virginia, and other applicable law](#) and [other WVU policies](#) including, but not limited to, policies documented at [http://oit.wvu.edu/oit/aboutoit/policy](http://oit.wvu.edu/oit/aboutoit/policy)/. The following uses of University IT resources are prohibited:

1. Interference or impairment to the activities of others, including but not limited to the following:
   o Creating, modifying, executing or retransmitting or otherwise using any computer program or instructions intended to obscure the true identity of the sender of electronic mail or electronic messages, such as the forgery of electronic mail or the alteration of system or user data used to identify the sender of electronic email; bypass, subvert, or otherwise render ineffective the security or access control measures on any network or computer system without the permission of the owner; or examine or collect data from the network (e.g., a "network sniffer" program).
   o Authorizing another person or organization to use University computer accounts or WVU network resources. Users are responsible for all of their accounts. Users must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of their account by unauthorized persons. Users must not share their password with anyone else or provide access to the WVU network resources to unauthorized persons.
   o Communicating or using any password, personal identification number, credit card number or other personal or financial information without the permission of its owner.
2. Unauthorized access and use of the resources of others, including but not limited to the following:

- Use of University resources to gain unauthorized access to resources of this or other institutions, organizations, or individuals.
- Use of false or misleading information for the purpose of obtaining access to unauthorized resources.
- Accessing, altering, copying, moving, or removing information, proprietary software or other files (including programs, libraries, data and electronic mail) from any network system or files of other users without prior authorization (e.g., use of a "network sniffer" program).
- Making unauthorized copies of copyrighted materials. Users should assume all software, graphic images, music, and the like are copyrighted. Copying or downloading copyrighted materials without the authorization of the copyright owner is against the law, and may result in civil and criminal penalties, including fines and imprisonment (see also Copyright Policy and Guidelines).

3. Damage or impairment of University resources, including but not limited to the following:
   - Use of any resource irresponsibly or in a manner that adversely affects the work of others, such as:
     - Hacking - attempting to obtain or use passwords, IP addresses or other network codes that have not been assigned to you or authorized for use as University employees, attempting to obtain unauthorized access to computer accounts, software, files, or any other University IT resources.
     - Malicious Activity - intentionally, recklessly or negligently damaging any system (e.g., by the introduction of any so-called "virus", "worm", or "trojan-horse" program); damaging or violating the privacy of information not belonging to the user; or misusing or allowing misuse of system resources.
   - Use of University resources for non-University related activities that unduly increase network load (e.g., chain mail, network games and spamming).
   - Any other activity not specifically cited above that may be illegal, harmful, destructive, damaging, or inappropriate use of University IT resources.

4. Unauthorized commercial activities, including but not limited to the following:
   - Using University resources for one's own commercial gain, or for other commercial purposes not officially approved by the University, including web ads.
   - Using University resources to operate or support a non-University related business.
   - Use of University resources in a manner inconsistent with the University's contractual obligations to suppliers of those resources or with any published University policy.

5. Violation of city, state or federal laws, including but not limited to the following:
   - Pirating software, music and images.
   - Effecting or receiving unauthorized electronic transfer of funds.

- o Disseminating child pornography or other illegal material.
- o Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose.
6. Using WVU computing resources to copy, download, upload, or share audio recordings, music, movies, videos, and other kinds of copyright-protected files without the owner's permission.
7. Using WVU computing resources to copy, download, upload, or share pornography is strictly prohibited. Violators are subject to disciplinary action as dictated by University policy and offenders may be subject to prosecution under federal and/or state laws.

### Security Obligation

- System Security: Access to information stored on the University's computers and network equipment is controlled by assignment of accounts and passwords. These accounts and passwords are controlled by the network manager and system administrators. This security information is the property of WVU.
- All University employees have an obligation to report security breach information to the network manager or system administrator. Failure to do so may result in disciplinary action. Any attempt to access, copy or modify this security information or to obtain system privileges to which employees are not entitled or any action which interferes with the supervisory or accounting functions of the systems or that is likely to have such effects will result in appropriate disciplinary action.

### De Minimis Usage

In the interest of making the use of IT resources a natural part of the day-to-day learning and work of all members of the University community, incidental personal use is tolerated. However, one should not use University sources of email, Internet access, and other IT services for activities of an extensive nature that are unrelated to University purposes. Excessive use of systems for recreational Internet browsing, email, or game playing is to be avoided and may subject University employees to disciplinary action up to and including termination.

### Enforcement

Although the University does not routinely monitor computer and network use, the University does reserve the right to monitor computer and network use for operational needs and to ensure compliance with applicable laws and University policies. The University considers any violation of this policy to be a serious offense and reserves the right to copy and examine any files or information contained on University systems or equipment that may be related to inappropriate use.

The Associate Provost, Office of Information Technology, also reserves the right to authorize disconnecting a user's account if the user represents a serious threat to system or email integrity. Violators are subject to disciplinary action as dictated by University policy. Users should also be aware that offenders may be subject to prosecution under laws including, but not limited to, the Privacy Act of 1974, The Computer Fraud and Abuse Act of 1986, National Stolen Property Act, The West Virginia Computer Crime and Abuse Act, and the Electronic Communications Privacy Act. The Associate Provost for Information Technology, the Assistant Vice President for Human Resources and/or Associate Dean of Student Life will be notified of infractions.

Suspected violations of this policy or related statute should be reported to the Office of the Associate Provost for Information Technology (OIT) in an email message addressed to: the Associate Provost, Information Technology or by calling 293-4874. In reporting a violation, complainants should cite the specific section of this policy that has been violated.

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

**Questions or Problems**

Questions, concerns or additional information about this and any OIT policy should be directed to the CIO office at **OIT_Admin@mail.wvu.edu**.

**Responsibility**

The Associate Provost for Information Technology (CIO) is the policy administrator for information technology resources and will ensure this process is followed. Additionally, Deans, Directors and Department Heads are responsible for compliance with University policy within their respective administrative areas.

# COPYRIGHT INFRINGEMENT POLICY AND GUIDELINES

## PURPOSE

To establish University policy on copyright protection that complies with applicable law and University policy.

### Scope

This policy applies to all University staff, faculty, administrators, officers and students (collectively, "users"), including those on the regional campuses and Extended Learning sites.

### Policy

It is the policy of West Virginia University to respect the copyright protections given by federal law to owners of digital materials and software, and to abide by all license and contractual agreements in the provision of resources and services to WVU.

Members of the campus community are advised to become as knowledgeable as possible regarding copyright law and this policy. Individuals who willfully disregard this policy and guidelines do so at their own risk and may be subject to personal liability. The University regards violation of this policy as a serious matter, and any such violation is without its consent and is subject to loss or restriction of computing privileges and disciplinary action up to and including termination, in the case of University employees, and expulsion, in the case of students.

### Violations and Prohibitions

It is against University policy for users to use University equipment or services to access, use, copy or otherwise reproduce, or make available to others any copyright-protected materials or software except as permitted under copyright law or specific license. Specifically, users are prohibited from:

- Copying or reproducing any licensed software on University computing equipment, except as expressly permitted by the software license. Also, users may not use unauthorized copies of software on University-owned computers or on personal computers housed in University facilities.
- Copying, downloading, or uploading audio recordings, music, movies, videos and other kinds of copyright-protected files electronically without the owner's permission.

- Posting copyrighted material on a WVU owned web site (official or personal).
- Additionally, faculty, staff, administrators and students must:
  - Fully read, understand, and abide by all terms of software license agreements.
  - Where applicable, remove any copyrighted material downloaded from the Web after the evaluation period has expired (WinZip, etc.)
  - Not accept unlicensed software from any third party.
  - Not install, nor direct others to install, illegal copies of computer software or unlicensed software onto any University-owned or operated computer system.
  - Comply with other University policies addressing copyright issues.

**Guidelines for Specific Materials**

*Computer Software*

- The software provided through the University for use by users may be used only on computing equipment as specified in the various software licenses.
- Users shall not make copies of university owned or licensed software except where and only to the extent explicitly permitted according to the terms of the applicable license and shall not use university hardware to make illegal copies of any copyrighted software for the purpose of selling, giving, or lending this software to others (including but not limited to software from the public and departmental computer labs) or for any other unauthorized purpose.
- Software that is purchased at a discount for classroom or other limited use shall be used only in the manner authorized by the seller (and removed or de-installed as directed).
- Users are responsible for knowing the license terms of any software acquired pursuant to a site license. The terms of site licenses vary, and software distributed under a site license must be used and copied in accordance with that license.
- Computer software known as "shareware" is under copyright protection. Individual users of this software are required to comply with all terms of any shareware license, including, where applicable, to register and pay for any software they retain and use.
- HSC Student Computer Program participants shall not make copies of software owned by the Health Sciences Center.
- Personally owned software may be used on the notebook computers; however, the software must pass the virus checking routines and recipient of the notebook must have proof of ownership before the software can be loaded to the computers hard-drive.

*Internet, WWW, Digital*

- Users shall not download copyright protected files from the Internet without permission from the copyright holder. These files could include MP3, wav, midi,

or other audio files; QuickTime, avi or other movie files; gif, jpeg or other picture files; as well as any other media files.
- Using [Peer to Peer (P-2-P) programs](#), such as [KaZaA](#) to distribute music, videos, etc. without copyright permission is against the [DMCA](#).
- The WVU high-speed network is a shared resource and primarily for academic use. The University reserves the right to revoke or restrict network access of individuals generating high network traffic which is not academically related (including but not limited to uploading and downloading copyright protected files).

## Enforcement

Although WVU [Network Services](#) does not routinely monitor the network for activity which is illegal or in violation of University policy, the University does reserve the right to monitor network use for operational needs and to ensure compliance with applicable laws and University policies. The University has a legal duty to comply with applicable laws protecting the intellectual property rights of third parties and to respond to formal legal complaints that it receives.

If a particular computer begins to consume excessive network resources, Network Services reserves the right to investigate and determine the cause for this excessive usage. Network Services can suspend, discontinue, limit or deny service without notice to anyone it determines is abusing the system. The [Associate Provost for Information Technology](#), the [Assistant Vice President for Human Resources](#) and/or [Associate Dean of Student Life](#) will be notified of infractions.

Suspected violations of this policy or related statute should be reported to the Office of the [Associate Provost for Information Technology](#) (OIT) in an email message addressed to: the Associate Provost, Information Technology or by calling 293-4874. In reporting a violation, complainants should cite the specific section of this policy that has been violated.

The University reserves the right to authorize removal of any illegal copyright material or disconnecting a user's account if the user represents a serious threat to system integrity or poses a liability to the University. The University may refer suspected violations of applicable law to appropriate law enforcement agencies.

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

## Questions or Problems

Questions, concerns or additional information about this and any OIT policy should be directed to the CIO office at **OIT_Admin@mail.wvu.edu**.

**Responsibility**

The Associate Provost for Information Technology (CIO) is the policy administrator for information technology resources and will ensure this process is followed. Additionally, Deans, Directors and Department Heads are responsible for compliance with University policy within their respective administrative areas.

## NOTEBOOK CUSTOMER SERVICE AND SUPPORT

## <u>POLICIES</u>

### <u>PURPOSE</u>

Health Sciences Center Information Technology Services (ITS) provides service and support for the Notebook computers through the ITS Support Services unit. The Support Services unit is located on the 2<sup>nd</sup> Floor of Health Sciences Center South, Room 2356. To reach the Support Services unit by phone, dial (304) 293-3631, or e-mail at HSC_helpdesk@hsc.wvu.edu.  Walk-ins are welcome.

### <u>POLICIES</u>

1.  The hours of operation for the ITS Support Services (HSC Help Desk) unit are as follows:

|  | **Fall / Spring Semester Schedule** | | **Summer Semester Schedule** |
|---|---|---|---|
| **Sunday** | CLOSED | | CLOSED |
| **Monday** | 8:00am – 6:00pm | | 8:00am – 5:00pm |
| **Tuesday** | 8:00am – 6:00pm | | 8:00am – 5:00pm |
| **Wednesday** | 8:00am – 6:00pm | | 8:00am – 5:00pm |
| **Thursday** | 8:00am – 6:00pm | | 8:00am – 5:00pm |
| **Friday** | 8:00am – 5:00pm | | 8:00am – 5:00pm |
| **Saturday** | CLOSED | | CLOSED |

Hours may vary during holidays and between semesters.

2.  The hours of operation for the ITS Learning Center Software Consultants are as follows.  Learning Center Software Consultants can provide assistance with software usage questions.  Online training is also available via SOLE.

|  | **Fall / Spring Semester Schedule** | | **Summer Semester Schedule** |
|---|---|---|---|
| **Sunday** | Varies | | Varies |
| **Monday** | 8:00am – 7:30pm | | 8:00am – 5:00pm |
| **Tuesday** | 8:00am – 7:30pm | | 8:00am – 5:00pm |
| **Wednesday** | 8:00am – 7:30pm | | 8:00am – 5:00pm |
| **Thursday** | 8:00am – 7:30pm | | 8:00am – 5:00pm |
| **Friday** | 8:00am – 5:00pm | | 8:00am – 5:00pm |
| **Saturday** | Varies | | Varies |

Hours may vary during holidays and between semesters.

3. The ITS Support Services unit can answer questions about your Notebook hardware and software.  If you have problems with your Notebook computer, please call or visit the Support Services unit.  Support Services unit technicians can diagnose and resolve hardware, software, and network connectivity problems.  If your computer requires hardware repair, an ITS technician will repair your notebook on-site when possible.  If the notebook cannot be repaired on-site, ITS will send your notebook to manufacturer for repair.   The Support Services unit has available a limited number of loaner notebook computers for use when your notebook is being repaired.
4. The ITS Support Services unit will make every attempt to correct hardware / software configuration problems on the notebook computers without changing custom configurations set up by the end-user.  If it is suspected that the end-user custom configuration is problematic, the notebook will be restored to original HSC configuration.
*5. Regular backups of your notebook computer are essential to ensure recovery of important data you have stored on your notebook.  It is your responsibility to back up important data off the notebook computer.  Backups can be performed using the DVD-RW or you can purchase a USB memory key or USB Harddrive for backup purposes.  As a friendly reminder, it is always good to verify your backups to ensure their integrity.

# NOTEBOOK NETWORK ACCESS

## GENERAL INFORMATION

### PURPOSE

The Health Sciences Center provides free Internet access to students at multiple locations within the Health Sciences Center and the WVU Residence Halls.

The Health Sciences Center provides "wireless" and "wired" network access within our facility for use with your notebook computer.

HSC "Wireless" Network Coverage areas include:
- Learning Center (all areas - including 1st floor study rooms)
- Student Lounge
- 7th and 8th floor classroom wings of Health Sciences South
- Classrooms 1106, 1107, 2157, 2094, 2116, 2118, 2149, 2162, 2165, 3016, 3022, 3067, 3084, 3129, 4007, 4023, 4080 located in Health Sciences North
- Classroom 1205 (Large OT Lab located on first floor HSS)
- Hostler Auditorium
- HSC Auditorium
- Cafeteria
- John E. Jones Conference Center
- Structural Biology Learning Center (SBLC)
- WV Room
- Charleston-Division Health Sciences Center
- Eastern-Division Health Sciences Center

HSC "Wired" Network Coverage areas include:
- Learning Center (1st floor lecture halls/ auditorium – all seats, 2nd floor - most student tables)
- 35 study carrels in the Student Lounge
- Cafeteria
- John E. Jones Conference Center
- Structural Biology Learning Center (SBLC)
- Classrooms on the 7th and 8th floor of Health Sciences South
- Classrooms 1107, 1901, 1905, 1909, 2094, 2116, 2157, 3016, 3067, 3084, 3129, 4007, 4023, 4080, and HSC Auditorium located in Health Sciences North
- Each room in the WVU Residence Hall

These points of access will provide unlimited Internet connectivity and access to medical reference resources available via HSC servers.

## NETWORK ACCESS POINTS / RESOURCES

1. The Learning Center is located on the 1st and 2nd floor of the north side of the HSC. 107 Windows-based PCs are available for use by students, faculty, and staff of the Health Sciences Center. All machines are connected to the HSC Computer Network, which provides direct Ethernet connectivity to the Internet. All hardware and software needed for connectivity is provided. Color and black & white Scanners and Laser Printers are available for use within the Learning Center. "Wireless" and "wired" network access is available throughout the Learning Center (including the 1st floor study rooms) for use with notebook computer or PDA. Lecture Halls and Auditorium on the 1st floor of the Learning Center have power and network connections at each seat. Various tables on the 2nd floor also have power and network connections for notebook users.

2. The Student Lounge is located on the ground floor of the north side of the HSC. "Wireless" access is available in this general area. Additionally, thirty-five study carrels have been connected to the HSC Computer Network for "wired" access – jack #1 at each study carrel has been activated for your use. This area provides direct Ethernet connectivity to the Internet and HSC resources. A HP Laser Printer is available for use within the Student Lounge.

3. The Cafeteria is located on the ground floor of the south side of the HSC. "Wireless" and "wired" network access is available in this area. Thirty-six "wired" network access points are available on the wall adjacent to the John E. Jones Conference Center within the cafeteria. This area provides direct Ethernet connectivity to the Internet and HSC resources.

4. The John E. Jones Conference Center is located on the ground floor of the south side of the HSC. "Wireless" and "wired" network access is available in this area. Forty-eight "wired" network access points are available for use for connection to the Internet and HSC resources, of which twenty-four access points are available from within John E. Jones Rooms 1, 2, and 3 and an additional twenty-four access points are located in the foyer.

5. The Anatomy department provides network access points in Rooms 4005 and 4023 of Health Sciences North. These rooms are part of the Structural Biology Learning Center (SBLC) which primarily serves students in specific Anatomy courses. Room 4005 provides twenty Windows-based PCs loaded with specific course-related software and is often scheduled for courses. Restricted access to the 4005 lab is sometimes available to other Health Sciences Center students. Room 4023 provides one hundred "wired" network access points and is also "wireless" accessible; it too is sometimes restricted for class use, but will be available to Health Sciences Center students during some hours. HP Laser Printers are available for use within the SBLC.

6. The 7th and 8th Floor classroom wings located in Health Sciences South provide "wireless" and "wired" network access points for students. All data jacks (wired) and wireless access have been connected to the HSC Computer Network, which provides

direct Ethernet connectivity to the Internet. HP Laser Printers are available for use on the 7$^{th}$ and 8$^{th}$ Floor classroom wings.

7. Classrooms 1107, 1901, 1905, 1909, 2094, 2116, 2157, 4007, 3016, 3067, 3084, 3129, 4080, and HSC Auditorium are located in Health Sciences North. Each seat within these classrooms has data and power outlets for use with your notebook computer. "Wireless" access is also available from these rooms. This connectivity provides access to the HSC Computer Network and the Internet.

8. Classrooms 1106, 2118, 2149, 2162, 2165, 3016, 3022, Hostler Auditorium, and OT Lab (1205) areas provide "wireless" access to the Internet and HSC resources.

9. To establish a connection in your Residence Hall room, pick up a HRLNet Network Connection brochure from your Residence Hall's Main Desk. This brochure contains an application form and general information about the HRLNet Network.

10. Most areas of our Charleston and Eastern Division Health Sciences Center facilities have "wireless" and "wired" network access points.

11. Dial-up SLIP/PPP service for off-campus access is available from WVNET for a fee of $16.95/month. WVNET provides full access to the World Wide Web, server space for personal Web pages, and local dialing from various geographical locations within West Virginia. WVNET's local calling area is available at: http://www.wvnet.edu/services/helpdesk/dialup_info/nfo5001.html.

# NOTEBOOK REMOTE ACCESS

## POLICIES

## PURPOSE

The professional and academic expectation is that each student shall maintain daily electronic contact with respective program and course work regardless of physical location.  Students can choose their own broadband or dialup service for the duration of their program, including coverage for any clinical rotations.

## POLICIES

1. The student is required to maintain daily electronic contact with respective program and course work regardless of physical location.
2. The student is responsible for arranging their own broadband or dialup service for the duration of their program.  All charges, including long distance and local access charges, are the sole responsibility of the student regardless of location.
3. Information Technology Services (ITS) highly discourages use of service providers that require using their software for access (ie. AOL, MSN).  Free dial-up providers should also be avoided due to spyware concerns.  ITS recommends Comcast cable modem, Verizon DSL, or WVNET dial-up as service provider options.
4. Technical support related to broadband or non-WVNET dialup service will be less of a priority at the HSC Support Services unit.

.

## NOTEBOOK BACK-UP

## <u>POLICIES</u>

### <u>PURPOSE</u>

Having a backup of important files and software stored on your Notebook is essential as even the most reliable computer is apt to break down eventually.  To avoid frustration caused by a computer crash resulting in loss of data, please backup your notebook computer on a regular basis.

### <u>POLICIES</u>

1.  Regular backups of your notebook computer are essential to ensure recovery of important data you have stored on your notebook.  It is your responsibility to back up important data off the notebook computer.  Backups can be performed using the DVD-RW or you can purchase a USB memory key or USB Harddrive for backup purposes.   As a friendly reminder, it is always good to verify your backups to ensure their integrity.

## ELECTRONIC MAIL

## POLICIES

## PURPOSE

University faculty, staff, students, and administrators are making extensive use of e-mail systems for access to colleagues and data sources. This policy establishes general guidelines and points to other resources and policies to be used / followed.

## POLICIES

1. WVU Health Sciences Center faculty and staff will use the student's WVU MIX e-mail address for all e-mail communications. It is the student's responsibility to ensure receipt of these communications. Due to the issues that follow, WVU only guarantees e-mail delivery to your MIX address. The Health Sciences Center strongly recommends that student MIX e-mail accounts not be forwarded to non-WVU e-mail accounts such as Hotmail, Yahoo, etc. due to system limitations with these and other non-WVU e-mail accounts. System limitations in non-WVU e-mail accounts may cause e-mail to not be delivered. Also, forwarding of MIX e-mail to a non-WVU e-mail account may result in the loss of class related communications and can cause "mail looping" which can create problems for your MIX e-mail account and subject your MIX account to suspension. If your MIX account is suspended, you continue to remain responsible for obtaining all class related communications. Failure to comply with this policy may result in missed communications of critical class work.

2. Electronic mail represents a conversation between you and another user. As such, the University will not attempt to regulate the content of your electronic mail and accepts no responsibility for the content of electronic mail. If you receive a piece of electronic mail that you consider offensive, you may direct your problem to the appropriate University Office. 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. While confidentiality cannot be ensured, all e-mail is considered private.

3. Mail Violations: In general, policies and restrictions outlined in state 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 Public Safety.

- 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, 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 severely.  Any other illegal use of electronic mail will also be dealt with severely and/or reported to the proper authorities.

## PROCEDURES

1. Suspected electronic mail violations should be reported to the University's E-Mail Help Desk via an e-mail message addressed to: e-mail@wvu.edu or by calling 293-4444.  In reporting a violation, complainants need to forward a copy of the suspected electronic mail message citing the specific section of this policy that has been violated.
2. The E-mail Help Desk complaint staff maintains a log of complaints in process, including status of each.  To inquire on the status of a complaint, please send your request to:  e-mail@wvu.edu with the subject listed as "Request for Complaint Status", or call 293-4444.
3. The E-Mail Help Desk complaint staff will assemble the available information on the complaint and process it in one of the following ways:
    - Student Complaint – If the complaint is against a WVU student, the information will be forwarded to the Office of Student Life.  Any student contact will be made by the Office of Student Life or by the Department of Public Safety.  The Office of Student Life will report back to the E-Mail Help Desk complaint staff with the status of the complaint upon resolution, or at least once a month.
    - Employee Complaint – If the complaint is against a WVU Employee, Office of Information Technology(OIT) will request that Public Safety carry out any further necessary investigations.  The OIT E-Mail Help Desk complaint staff will then forward the complaint, along with recommended action, to the Associate Provost, Office of Information Technology.  The Associate Provost, Office of Information Technology will be responsible for final resolution of the complaint.

- Unsubstantiated Complaint – If there is no evidence to support the complaint and the complaint can not be substantiated, the complaint will be closed with no further action.

The Associate Provost, Office of Information Technology reserves the right to authorize disconnecting a user's account if the user represents a serious threat to system or mail integrity. As part of an investigation, the Associate Provost, Office of Information Technology (or his designee) may examine mail files, logs, and any other appropriate documents or testimony. Any necessary disciplinary action shall be determined by the appropriate Faculty, Staff or Student Handbook, state or federal law.

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.

**NOTEBOOK NETWORK PRINTING**

**POLICIES**

**PURPOSE**

The Health Sciences Center provides computer and printing resources for student use at various locations within the Health Sciences Center.  This policy establishes a uniform policy for printing at these locations.

**POLICIES**

1.  The computing resources within the Health Sciences Center are intended to be used for West Virginia University related work only.  Persons misusing computing resources are subject to disciplinary action in accordance with the Employee, Faculty, and Student Handbooks.
2.  Faculty, staff, and students are encouraged to utilize computing resources in a responsible and appropriate manner.
3.  In order to control the steadily increasing costs associated with laser printing, users will be charged $0.06 per sheet for black and white laser printing and $0.25 per sheet for color laser printing.  Please note duplex printing costs $0.12 per sheet for black and white laser printing and $0.50 per sheet for color laser printing.

**NOTEBOOK INVENTORY**

**POLICY**

**PURPOSE**

This policy is established so that West Virginia University Health Sciences Center and notebook manufacturer can accurately track HSC Student Computer Program notebook computers for warranty/insurance claims purposes.

**POLICY**

1.  Serial numbers of all hardware and software components issued to students, faculty, and staff will be recorded in the HSC Student Computer Program Asset Management database.  In the event a hardware component is replaced due to hardware failure, it is the responsibility of the student, faculty, or staff to report the change so that database integrity can be maintained.   This information must be reported to HSC Information Technology Services; Support Services unit / 2$^{nd}$ Floor Health Sciences South or (304) 293-3631.

## NOTEBOOK TRAINING MATERIALS

## <u>POLICY</u>

### <u>PURPOSE</u>

This policy protects West Virginia University Health Sciences Center from unauthorized use and copying of training materials provided in electronic and hard copy format.

### <u>POLICY</u>

1. All training documentation provided with the Notebook is the property of West Virginia University Health Sciences Center.  The user shall not copy, edit, or distribute any training documentation provided, unless otherwise indicated.

## HSC STUDENT COMPUTER PROGRAM COORDINATORS

The HSC Student Computer Program Coordinators are responsible for overseeing implementation of the Student Computer Program for students in their respective school or program.  Your coordinator will serve as an information resource and will provide guidance throughout the program.

| School / Program | Coordinator | Phone | Email |
|---|---|---|---|
| Dentistry | Charles Groff | 293-1567 | cegroff@hsc.wvu.edu |
| MD Program | Pamela Carico | 293-2409 | pcarico@hsc.wvu.edu |
| Nursing Program | Kim McCourt | 293-1927 | kmccourt@hsc.wvu.edu |
| Professional Programs<br>-Physical Therapy<br>-Occupational Therapy<br>-Pathologist's Assistant | April Cukic | 293-1320 | acukic@hsc.wvu.edu |
| Pharmacy Program | Mary Stamatakis, PHARMD | 293-1466 | mstamatakis@hsc.wvu.edu |
| Public Health | Leah Adkins | 293-1097 | ladkins@hsc.wvu.edu |

## LOANER EQUIPMENT

## <u>POLICIES</u>

### <u>PURPOSE:</u>

The Health Sciences Center has implemented a loaner equipment return policy to ensure loaner equipment is returned in a timely manner for distribution to other students in need of loaner equipment.  Students in non-compliance of this policy will be subject to the following.

### <u>POLICIES:</u>

1. Students receive up to two notifications for failure to return the loaner with a notice that "failure to return may result in denied registration with Admissions/Records." This restriction is at the Program Coordinator's discretion.
2. The restriction includes registration and transcript requests.
3. The student shall be assessed a late fee of $50.00.