The OU Health Sciences Center CAH Student Computing Policies & Procedures 2018 - 2019 is a PDF document with embedded bookmarks. Simply click on the main heading or section number on the Table of Contents or Index.

Please note, the information contained in this handbook may change from time to time by action of appropriate segments of the University.

CAH Student Computing Policies & Procedures 2018 - 2019

The University of Oklahoma Health Sciences Center

EQUAL OPPORTUNITY STATEMENT

The University of Oklahoma is an Equal Opportunity Employer. To find out more visit: http://www.ou.edu/content/web/landing/legalnotices.html

UNIVERSITY OF OKLAHOMA HEALTH SCIENCES CENTER
Generated: 8/14/2019 7:58:39 AM August 2017

Table of Contents

1 - THE BASICS

1.1 - Computers

All College of Allied Health students admitted for the academic year 2018-2019 shall possess a laptop computer for access to a wide variety of educational materials and resources. Educational pricing for computers and software is available through HSC IT Support Services at (405) 271-8664 (Ask for Jeff McCanlies, or Leslie Sausins) or you may inquire at the Student Union computer service desk, (405) 271-2203 or toll-free (888) 435-7486.

1.2 - Network Access

All COAH students have OUHSC domain accounts and therefore have access to a variety of campus computing resources. Any student who does not have an OUHSC domain account should have one created by completing a New User Account Request form. This form can be printed from the IT service desk web site. Fill out the form and submit it to the Office of Academic and Student Services (OKC AHB 1009; Tulsa 2J12) for account sponsor signature and forwarding to Information Technology. A new OUHSC domain user account will be created with a pre-expired password and will be forwarded to the account sponsor and/or IT service desk in 24-72 hours. A pre-expired password is one that will expire after being used the first time. The student will be presented with a screen to change their password. Passwords must conform to password complexity rules as outlined in section 5.1.

What HSC applications require two-factor authentication?

- Employee self-service access from off-campus
- Student self-service access from off-campus
- VPN (connect.ouhsc.edu)
- Direct deposit from either off-campus or on campus

How does two-factor authentication work?

Once you've enrolled in OUHSC's two-factor authentication system, you will login to protected applications as usual with your HSC User ID and password. If you are off-campus (or on campus for some services), you will be prompted to send a request for authentication to the smartphone or tablet you registered here. Approve the login from the smartphone or tablet, and the webpage on your computer will automatically refresh to the location you are attempting to reach.

What is considered off-campus?

Off-campus would include your home internet connection, public internet locations, connectivity via the HSC connect.ouhsc.edu VPN service, or even cellular data connectivity regardless of physical location. Only dedicated HSC wired and wireless networks are considered to be on-campus for two-factor authentication.

1.3 - E-mail

The University's electronic mail system allows faculty, staff and students to write, send and receive email communications. The email system is owned by the University and maintained to facilitate business communications. **Students should keep in mind that personal views, opinions, and philosophies expressed in personal email should be identified as such to avoid the perception they are speaking on behalf of the University.** It is not proper use of general or mass mailings to send messages with content that is political, religious, commercial, chain letters, hoaxes, editorials, poetry, etc…. **for example, just as it is prohibited for a University employee or student to use University facilities, equipment or letterhead to engage in political activities, it is equally improper and strictly prohibited to use the campus email system for political purposes. Communication of unauthorized, confidential or copyrighted material is also strictly prohibited without prior approval**. For additional information please review the document entitled "Acceptable Use of Information Systems at The University of Oklahoma Health Sciences Center" located here.

To avoid a possible security breach and downloading of computer viruses or worms, **the OUHSC Exchange email system is the only supported email platform for the campus network** (use Outlook and/or the HSC webmail interface ONLY. The Exchange email system provides necessary antivirus capabilities that may not be present though third party e-mails providers (yahoo, gmail, hotmail, etc). **Therefore, do not use third party email providers when you are using a computer on campus OR from your home computer when connected to the campus network.**

Refrain from using "wallpaper" or decorative images on email messages. This unnecessarily increases the size of the file, appears as an attachment and often reduces the legibility of the overlying text message.

1.4 - Prohibiting Forwarding of OUHSC Email

Auto-forwarding, forwarding, re-directing, or sending, receiving confidential or sensitive OUHSC information from OUHSC accounts to external, private email accounts is strictly prohibited. In addition, the auto-forwarding function will be disabled.

Transmission of Confidential or Sensitive Email

If confidential or sensitive OUHSC information, including but not limited to PHI, must be transmitted to a non-University email account or over an external network (e.g., the Internet), the message must be encrypted. Encryption options include typing [secure] in the email subject line, using the Proofpoint Secure Email plug-in for Outlook, and sending via a patient portal. (For sending PHI via email, refer to HIPAA Privacy Safeguards policy.)

Secure File Transfer allows HSC users to securely send or receive files that exceed the 50 MB attachment size limitations of the campus email system. Secure File Transfer also helps safeguard the confidentiality and integrity of sensitive data in compliance with HIPAA and other regulatory requirements. The integrated encryption protects sensitive data from unauthorized access during electronic transmission. Secure File Transfer can be accessed here.

Users may send confidential or sensitive University information via encrypted email only from their ouhsc.edu account and only to authorized recipients. For example, PHI may be sent only for treatment, payment, or operations purposes and to third parties with whom the University has a Business Associate agreement in place (contact Purchasing or the Office of Research Administration to confirm).

Individuals must not send, forward, auto-forward, re-direct, or receive confidential or sensitive OUHSC information through non-OUHSC email accounts. Examples of non-OUHSC email accounts include, but are not limited to, Gmail, Cox mail, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).

Emails that contain confidential or sensitive OUHSC information, such as PHI or regulated data, must include a confidentiality notice at the end of the correspondence, such as: *Confidentiality Notice: The information contained in this message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure, distribution, or retention is strictly prohibited. If you are not the intended recipient, or believe that you have received this message in error, please notify the sender immediately by reply email and delete the original message.*

Please be advised that monitoring of your computer system, email accounts, domains and servers may be necessary to detect, prevent and eradicate illegal or otherwise damaging use by internal and external users of the University computer network in order to protect the security and integrity of the University computer system. Such monitoring efforts could lead to the imposition of criminal and civil penalties to those users whose actions are illegal, unlawful, damaging, or threatening to the University computer systems. If you need additional information on OU's security efforts/policies, please visit the Information Technology website.

1.5 - Remote Network Access

Users needing to access OU services, such as file servers (does not apply to HSC Webmail), from off campus are required to enter the University network through the VPN. Each time you want to use secured OU services from off campus, you must connect to your Internet Service Provider and then start and authenticate through the VPN client.

All PC's connecting to the university network (including home computers attaching through VPN) are required to:

- Install and use antivirus protection.
- Set all "auto updates" (security patches and antivirus updates) to occur daily while the PC is on and actively connected to the Internet.
- Enable the firewall that comes with the operating system.

2 - COMPUTER REQUIREMENTS FOR STUDENTS ENTERING THE COLLEGE OF ALLIED HEALTH

All College of Allied Health students admitted for the academic year 2017-2018 shall possess a laptop computer for access to a wide variety of educational materials and resources. The privacy and security of the protected health information (PHI) governed by federal HIPAA law and monitored by the Office of Civil Rights (OCR), is of critical importance to the entire OU

Health Sciences Center community. As a result, All laptop computers used for university related activities, including academic course work, testing, classroom notes, HSC email, and clinical or research activities MUST complete a device security clinic prior to their use with any HSC resources.

Rationale for computer requirements

The trend in health care is more computer usage in daily practice and the trend in education is to require more computer and technology usage in instruction and in the classroom. The need for proficiency in the use of computers in research is well established. Demands of the clinician, educator and researcher brought about by the explosion in technology and information of the 1990's necessitates computer literacy to increase the personal and professional effectiveness of the College of Allied Health graduates. **Effective starting the fall 2007 semester, the College instituted a laptop computer requirement upon admission.**

Our campus provides a broad distribution of wireless network coverage for campus users and guests compatible with **802.11b/g/n protocols** which work with standard integrated internal or PCMCIA external wireless network cards. Therefore, students **should not use** an internal or external **mobile** broadband card (these devices act like cell phones and require an activation plan) to establish a wireless connection. In fact, broadband wireless cards interfere with microphones in our videoconferencing classrooms. Therefore they must be turned off during class, just like cell phones.

Some students entering the College my already have a laptop computer. There may be an instance where a laptop may be too old to accommodate required software. If a student finds some software runs too slowly or not at all, a new laptop purchase should be considered.

2.1 - Optional peripheral devices to consider

- Printer/scanner
- Surge protection power strip (UL 1449 rating, 330-400v suppression, Protection LED indicator)
- External USB drive (primarily for data backup): Encryption will occur when used on encrypted laptop computer.
- External DVD burner (if the computer does not have one built in)

If you wish to have Internet access at home, check with Cox Communications , AT&T DSL, or other internet provider.

Additional instructions, account usernames, and passwords will be distributed prior to Orientation.

3 - FUNCTIONAL SOFTWARE EXPECTATIONS FOR ALLIED HEALTH STUDENTS

Students come to the College of Allied Health with varying degrees of depth and breadth of computing knowledge, abilities, and experience. Given this, we ask that you as a new member of the College familiarize yourself with our functional software expectations and assure that you meet or exceed our minimal standards. Moreover, please recognize that technology in its various forms is a powerful tool that can both enhance and detract from your learning. As such, please consider the professional responsibility you have to your academic success by using technology in thoughtful and positive ways. Just as you will grow as a practitioner in your chosen profession, so should your use of computing technology reflect this maturation process.

To avoid a possible security breach and downloading of computer viruses or worms, **the OUHSC Exchange email system is the only supported email platform for the campus network** (use Outlook and/or the HSC webmail interface ONLY. The Exchange email system provides necessary antivirus capabilities that may not be present though third party e-mails providers (yahoo, gmail, hotmail, etc). **Therefore, do not use third party email providers when you are using a computer on campus OR from your home computer when connected to the campus network. Auto-forwarding, forwarding, re-directing, or sending, receiving confidential or sensitive OUHSC information from OUHSC accounts to external, private email accounts is strictly prohibited. In addition, the auto-forwarding function will be disabled.**

Following is a checklist for student self-evaluation. All items in Part I should initially be completed before your first semester and then continue to be maintained. You should complete Part II by the end of your first semester. If you need help learning to perform any of these tasks, we suggest you use resources in the following sequence:

1. Use program specific “Help”.
2. Search the Internet for assistance. We suggest using “function name + tutorial” in the search box.
3. Contact ouhsc.edu IT Service Desk at 405.271.2203 (OKC), 918.660.3550 (Tulsa) or 888.435.7486 (toll-free) Monday-Friday 8am-5pm.

3.1 - Part 1

- Verify installation & version number of all required software
- Verify proper configuration of wireless connectivity on-campus to HSCSTUDENT.
- Schedule & verify auto-updates of all required software. **Schedule for daily updates.**
- Activate "update now" feature in antivirus software
- Open & use all required software
- Save, rename & delete files
- Reinstall "Lockdown Browser" software prior to each semester & additionally as directed
- Verify proper operation of "Lockdown Browser" software prior to each online exam or quiz
- Access & use ouhsc.edu webmail, including the following:

  – Open, read, close & delete email messages
  – Open, read & save incoming email attachments
  – Attach & send outgoing email attachments (Light version works best for attachments)
  – Create & reply to an appointment or meeting request
  – Create a new contact & a distribution list
  – Add an appropriate and professional e-mail signature
  – Create, activate & deactivate an auto-reply in the "out-of-office" assistant option

- When using MS Word & MS PowerPoint

  – Insert symbols, images, graphics, shapes, arrows, text boxes, charts & video clips
  – Arrange, rotate, crop, resize & change attributes on text boxes, shapes & graphics
  – Insert pages or slides from a different file of the same type
  – Insert & remove website URLs
  – Verify / test inserted URLs and video clips
  – Demonstrate the ability to use the following commands & features

    – Copy, cut & paste text, using menu & keyboard shortcuts
    – Modify font theme, size, color, superscript & subscript
    – Modify page setup, margins, indents, tabs & bullets
    – Add, modify & delete page numbers, headers & footers
    – Use select all, find, replace, undo & redo
    – Turn ruler & gridlines on/off
    – Create, format, modify & delete tables
    – Use spell checker, grammar checker & thesaurus
    – Change document views, zoom in & out on document
    – Track, accept & decline changes (Track changes to document in MS Word)
    – Use navigation pane in MS Word, including copy, paste & move pages
    – In MS PowerPoint

      – Change slide design, background color & hide background graphics
      – Setup and activate Slide Show in MS PowerPoint
      – Use slide sorter in MS PowerPoint, including copy, paste & move slides

- When using browser

  – Successfully use basic internet search tools (Google, Bing, etc)
  – Clear history, cache and/or cookies
  – Differentiate between search engines, opinion websites, patient education websites & primary research-based websites and their content
  – Recognize features that contribute to website content credibility
  – Accurately cut & paste website URLs

- Other

  – Zip, open & unzip files
  – Connect your computer, tablet or Smartphone to a wireless network
  – Access and use Proofpoint Secure File Transfer website for transferring large or multiple files

3.2 - Part 2

You will be expected to develop the following competencies early in your program of study. Becoming familiar with these tools and resources prior to beginning your program or during your first semester will be beneficial and improve your efficiency when using these tools to complete course assignments:

- Successfully access and use Library search tools and e-resources

  – Access from both on-campus and off-campus computers (use "Proxy server page" when off-campus)
  – Identify, search, refine searches & retrieve citation references from OVID, EBSCO & public databases, including using Boolean logic (operators) in your search strategies

    – CINAHL
    – ERIC
    – MEDLINE
    – PUBMED
    – Google Scholar

  – Retrieve electronic versions or photocopies of full-text reference articles from

    – E-resources
    – Print references (shelved in libraries)
    – Document Delivery

      – Interlibrary loan
      – Create an ILLiad account so when you need it, you are ready "to go"

  – Identify & access evidence-based practice e-resources

    – EBM Review: Cochrane Database of Systematic Reviews
    – Dynamed
    – UpToDate
    – Natural Medicines

  – Identify & access online textbook & reference collections

    – AccessMedicine
    – Books@OVID
    – STAT!Ref
    – Merck Manual

  – Manage full-text references and citations

    – Select a tool available for free through the library

      – Ref Works, a web-based account, very user friendly
      – EndNote, more robust & appropriate for theses or dissertation tracks
      – Reference Manager, more robust & appropriate for theses or dissertation tracks

3.3 - Required Software

Students entering the College will need certain software installed and functioning on their computers in order to satisfy requirements of their respective programs.

Some educational programs required additional specific software programs such as SAS (a statistical analysis program). SAS does not run on a Mac computer, but can be loaded if virtual-PC software is installed on a Mac. Regardless of your computer hardware, each student needs to realize that they may need to purchase and install additional software during their educational program. The IT Service Desk is available to assist with software installation and configuration, but is not staffed to provide "instant" service.

3.3.1 - Mac (macOS 10.12 or higher)

Desire2Learn course management software

- Test your Browser. This test will check all required components and optional components for your computer. Visit this link for a direct testing of your browser
- Recommended browsers for D2L:
    - Chrome
    - Firefox
    - Safari for Mac

The latest version of Java
Download the latest version

VLC Media Player

Apple uses the Preview app for its PDF reader/editor

Apple Computer supplies their own software updates
Use the Software Update feature (available on the Apple menu) to check that you have the most up-to-date version of software.

Device Security Clinic

The risks of identity theft, compromised accounts, and data loss are real threats that require a particular focus for healthcare organizations such as the OU Health Sciences Center. The protection of our patient, student, and employee information is our primary concern. OUHSC recognizes this responsibility and is taking the initiative to provide you, our patients, and all OUHSC community members with a comprehensive approach to security practices and technologies.

Therefore, in order to protect your devices and meet federal requirements for accessing any network which contains protected health information, all student devices used to connect to OUHSC resources (including Email or Web Mail) are required to complete the Device Security Clinic (DSC) and use the OUHSC Security Software Suite. This software is free for your use while you are a student here and will provide your personal devices with up-to-date data encryption, anti-virus capabilities, and other security tools needed to protect your devices and the data they may contain.

Accessing HSC Resources Requires a Secure Device: What does this mean for me?

This means that your device(s) will be protected (as much as possible) from threats and data loss. This will be done by using the OUHSC Security Software Suite. The patches and antivirus soft-ware will aid in preventing cyber-attacks, and the data encryption software will aid in preventing data loss and identity theft in the event your device is lost or stolen. This software is free to you.

More Information about the Device Security Clinic

When instructed - Click here to schedule your Device Security Clinic Appointment

Anti-Virus software
Your computer will have an Anti-Virus software installed as a part of the Device Security Clinic . For more Information on your Anti-Virus Software please see this site or contact the Service Desk for more information.

LockDown Browser for online exams
This must be checked prior to exams and reinstalled if necessary.

Installing the software

- Under the Terms & Conditions select “Install Now”
- The browser will begin the download
- Download should automatically start. If it doesn’t select the “click the link” to download manually.
- Open the dialog box to run software
- Select Run from the dialog box
- Select install software
- Accept License agreement
- Software is now downloaded
- Select Finish from Respondus window
- Close browser window
- You should now see the lockdown browser icon on your desktop
- Open D2L and test your access to D2L courses. Take an example test again if one is available to you. You will see “launch Lockdown Browser” at the bottom of the exam.
- Trouble Shooting Suggestion: If Respondus LockDown Browser is not working properly with your D2L, completely uninstall

the software, restart your computer, and try installing it again.

If you need more assistance, please contact the ISS Dept. (Office room number AHB 2053)

Note: Please check Lockdown Browser before each exam to make sure software is working correctly.

If you need more assistance, please contact the ISS Dept. (Office room number AHB 2053). Note: Please check Lockdown Browser before each exam to make sure software is working correctly.

Office 2016
You can obtain a free version at the link above. For assistance visit the IT Service Desk located in Rm 105 of the Student Union, 405.271.2203 (OKC), 918.660.3550 (Tulsa) or 888.435.7486 (toll-free) Monday-Friday 8am-5pm.

3.3.2 - PC (Windows 10 or higher)

Desire2Learn course management software

- Test your Browser. This test will check all required components and optional components for your computer. Visit this link for a direct testing of your browser
- Recommended browsers for D2L:
  - Chrome
  - Firefox

Java
Download the lates version

VLC Media Player

Adobe PDF Reader
Download the latest version

Make sure you have installed all windows updates.
This will ensure that your computer is running the necessary components needed for all required programs.

Device Security Clinic

The risks of identity theft, compromised accounts, and data loss are real threats that require a particular focus for healthcare organizations such as the OU Health Sciences Center. The protection of our patient, student, and employee information is our primary concern. OUHSC recognizes this responsibility and is taking the initiative to provide you, our patients, and all OUHSC community members with a comprehensive approach to security practices and technologies.

Therefore, in order to protect your devices and meet federal requirements for accessing any network which contains protected health information, all student devices used to connect to OUHSC resources (including Email or Web Mail) are required to complete the Device Security Clinic (DSC) and use the OUHSC Security Software Suite. This software is free for your use while you are a student here and will provide your personal devices with up-to-date data encryption, anti-virus capabilities, and other security tools needed to protect your devices and the data they may contain.

Accessing HSC Resources Requires a Secure Device: What does this mean for me?

This means that your device(s) will be protected (as much as possible) from threats and data loss. This will be done by using the OUHSC Security Software Suite. The patches and antivirus soft-ware will aid in preventing cyber-attacks, and the data encryption software will aid in preventing data loss and identity theft in the event your device is lost or stolen. This software is free to you.

More Information about the Device Security Clinic

When instructed - Click here to schedule your Device Security Clinic Appointment

Anti-Virus software
Your computer will have an Anti-Virus software installed as a part of the Device Security Clinic . For more Information on your Anti-Virus Software please see this site or contact the Service Desk for more information.

LockDown Browser for online exams
This must be checked prior to exams and reinstalled if necessary.

Installing the software

- Under the Terms & Conditions select "Install Now"
- The browser will begin the download
- Download should automatically start. If it doesn't select the "click the link" to download manually.
- Open the dialog box to run software
- Select Run from the dialog box
- Select install software
- Accept License agreement
- Software is now downloaded
- Select Finish from Respondus window
- Close browser window
- You should now see the lockdown browser icon on your desktop
- Open D2L and test your access to D2L courses. Take an example test again if one is available to you. You will see "launch Lockdown Browser" at the bottom of the exam.
- Trouble Shooting Suggestion: If Respondus LockDown Browser is not working properly with your D2L, completely uninstall the software, restart your computer, and try installing it again.

If you need more assistance, please contact the ISS Dept. (Office room number AHB 2053)

Note: Please check Lockdown Browser before each exam to make sure software is working correctly.

If you need more assistance, please contact the ISS Dept. (Office room number AHB 2053). Note: Please check Lockdown Browser before each exam to make sure software is working correctly.

Office 2016
You can obtain a free version at the link above. For assistance visit the IT Service Desk located in Rm 105 of the Student Union, 405.271.2203 (OKC), 918.660.3550 (Tulsa) or 888.435.7486 (toll-free) Monday-Friday 8am-5pm.

4 - LAPTOP HARDWARE REQUIREMENTS / RECOMMENDATIONS

4.1 - PC Laptop Hardware Requirements / Recommendations

Laptop Hardware Requirements / Recommendations

Component	**Already Owned Laptop Minimum Requirements (Consider Upgrading)**	**Recommended New Laptop Purchase Specifications**	**COAH IT Recommended** ***Laptop Speed Machine***
Processor (CPU)	5th Generation Intel Core i3	Current Generation (8th) i3 or better	Current Generation (8th) i7
Memory (RAM)	4GB	8GB+	16GB – DDR4 Ram.
Internal Storage	Traditional Hard Disk or Solid State Drive	Solid State Drive	PCIe M.2 Solid State Drive
Wireless Network Adapter	802.11n	802.11ac	802.11ac
Operating System	Windows 10 Pro, Education	Windows 10 Pro, Education	Windows 10 Pro, Education
External Storage	USB 2.0 Flash or External Disk Drive	USB 3.0 Flash or External Disk Drive	USB 3.1 Flash or External Disk Drive

4.2 - Mac Hardware Requirements / Recommendations

Mac Hardware Requirements / Recommendations

Component	**Already Owned Mac Minimum Requirements** **(Consider Upgrading)**	**Recommended New Mac Purchase Specifications**	**COAH IT Recommended** ***MacBook Pro Speed Machine***
Date of Manufacturer (Use About this Mac)	Mac Book/Air/Pro, Early 2016	Mac Book/Air/Pro, 2018	MacBook Pro, 2018
Processor (CPU)	Intel Core m3 Processor	Intel Core i5 Processor (7^{th} gen)	Intel Core i7 Processor (7^{th} gen)
Memory (RAM)	4GB	8GB+	16GB
Internal Storage	Traditional Hard Disk or Solid State Storage (SSD)	Solid State Storage (SSD)	Solid State Storage (SSD)
Wireless Network Adapter	802.11n	802.11ac	802.11ac
Operating System	El Capitan or Sierra	High Sierra	High Sierra
External Storage	USB 2.0 Flash or External Disk Drive	USB 3.0 Flash or External Disk Drive	USB 3.1 Flash or External Disk Drive

5 - FILE STORAGE, BACKUP AND SECURITY

5.1 - File Storage and Passwords

All student users authenticate to the OUHSC domain for access to network resources (i.e. printers, file servers). Proper user names and passwords are required for this access. OUHSC domain passwords expire every 90 days and require the user to change their password at that time. The user will automatically be notified at least 14 days prior to password expiration. You may also change your password more frequently. **Passwords must be at least 8 characters in length and must contain a combination of uppercase and lowercase letters, numbers, and special characters** such as /!@#$%^&*(+)-~`{}[;':"]?><. Click here for more information about changing your password. **Do not share passwords with anyone. If you think someone knows your password, change your password immediately.**

Files created by users should be stored on portable encrypted storage medium (disk, CD, USB drive, etc.) or by using OU Sync & Share service. See Appendix IV for information on signing up and using OU Sync & Share. Files are not to be stored on the local hard drive of College or campus computers. The only exception is temporary storage of PowerPoint or image files for use during a classroom presentation. **Do not store PHI from patients on portable storage media or on your personal computer.**

More information about accessing network files and folders is provided in Appendix II.

5.2 - Server Data Backup

All mission critical servers are designed with power and hard drive redundancy to prevent serious failures. The servers are backed up every workday.

5.3 - Daily Security Procedures for Users

In addition to following the procedures for complex passwords and other security measures discussed in this manual, users should adhere to the following on a daily basis.

All notebook computers should be set to use password-enabled screen savers (only system or other approved screen saver). This feature will reduce the risk of file tampering and file theft when the student is away from their computer.

Computer printed material that is of a sensitive or confidential nature should be removed from printers immediately after printing and should be stored in a lockable, secure area such as a locked desk drawer or a locked file cabinet. If the printed material becomes outdated or otherwise obsolete, it should be destroyed in a manner sufficient to render it illegible. Contact your department to determine if shredders are available for student use.

6 - PRINTING

Students may choose to use any available printing services. To save on printing costs, here are some suggestions for more efficient or alternative printing solutions:

- 2-up printing - Two pages side by side on 8.5" x 11" page
- 4-up printing - Four pages on 8.5" x 11" page
- Canceling print jobs at PaperCut release station, Go-Print kiosk or at desktop
- Print only what you need
- Printing at home

6.1 - College PaperCut Printing Services in Oklahoma City

The "PaperCut" system (similar to the system in use in the Student Union) is the printing solution in AHB 2040. This pay-to-print system offers only monochrome (black and white) printing. Specific printing instructions are provided at the PaperCut release station (AHB 2040). **Students will be required to pay for print jobs at $.05 per page.** Printing is available via the web. This web interface also allows for adding funds to your PaperCut account. To print via the web, follow these steps:

1. Connect to the HSCSTUDENT Wi-Fi network.
2. Browse to this website
3. Login with your OUHSC credentials.
4. Select Web Print from the left hand menu.
5. Select "AHB2040-Dell5210n_papercut " printer.
6. Click next to choose how many copies. Then click Next.
7. Select your document and click Upload & Complete!
8. Go to the Papercut release station in room 2040 to login and release your documents to print.

6.2 - Library Go-Print Services in Oklahoma City

The Library Go-Print service is not the same as the PaperCut printing service. Go to Library, 3rd floor reference desk to activate or add value to a "Library Go-Print card". This system is different to accommodate use of printers and copiers by non-OUHSC Library clients.

6.3 - Printing Services at OU-Tulsa

Printers in the OU-Tulsa Student Computing Lab, room 1C65, are available for use by students.

7 - VIRUS PROTECTION

7.1 - Virus Protection Software and Operation

All workstations must have approved virus protection software installed and running at all times. The virus protection software checks the hard drive boot sector and system critical files at boot-up. This software checks removable media (diskettes, CD's, flash drives) upon their insertion and opening of files. The software also automatically checks files as they are downloaded from the Internet.

Virus definition files should be automatically updated daily and each hard drive should automatically be scanned weekly. This is accomplished using the "scheduler" feature of the virus protection software (set by user).

The CIS staff or IT Service Desk should be contacted immediately when any of the following occur (as listed in Appendix

V):

- If a virus is detected by the computer,
- If a user suspects their computer is infected with a virus,
- If the computer is demonstrating odd, erratic or strange behavior, or
- Whenever a user receives a virus alert via email from non-OUHSC entity.

The CIS staff also recommends the use of Malwarebytes product in the free or full-feature version (cost ~ $49.99), as additional protection for your computer.

7.2 - Determining if a Virus is Real or a Hoax

Many email virus alerts are actually hoaxes. Responding to or forwarding these email messages wastes time and resources. **If the DCIS is not available, the user should check the Threat Explorer at Symantec's web site to determine if the alert refers to an actual virus or a virus hoax.** All credible virus alerts should be forwarded to the DCIS: Derek Teague and Campus Network Security: Randy Moore immediately. Hoax alerts should not be forwarded, but instead deleted from your email inbox.

8 - SPECIAL EQUIPMENT RESOURCES

Specialized audio-visual and computer equipment in AHB and OU-Tulsa classrooms are shared among the Programs and Colleges. Computer equipment, DVD/VCR's, TV monitors, desktop presenters, and video-data projectors are available in AHB & OU-Tulsa classrooms. Full-motion videoconferencing equipment is integrated with the audio-visual systems in several classrooms on both campuses.

9 - TRAINING AND SUPPORT

9.1 - Expectations

Students are expected to learn to use software applicable to their program of study. The College provides some user-education seminars and computer-related periodicals. User education seminars are available on campus each semester, some are free and others are fee-based. Some departments also have user manuals available for a variety of software. Students are expected to utilize on-line help resources provided with applications whenever possible. All College computers have Internet access to accommodate searches for specific problem resolution. If a student suspects a malfunction or misconfiguration in any software, they should immediately contact the system administrator Derek Teague at 405.271.2288 or 405.271.8001 ext. 43412. The University maintains an IT Service Desk available to all users to answer many questions relating to the specific operation of most major office software. The IT Service Desk phone number in OKC is 405.271.2203. Toll-free number for the IT Service Desk is 888.435.7486. Please refer to the IT Service Desk webpage for hours of operation.

9.2 - Course Management Systems

Campus faculty, staff and students, are increasingly using course management systems. Each College has personnel assigned to provide faculty, staff and students with assistance getting started using course management systems (as listed in Appendix V):

- OUHSC Desire2Learn
- College of Medicine Hippocrates

10 - DISASTER RECOVERY

Disasters, which can threaten property and data, include but are not limited to fire, flood, vandalism, theft, hardware failure, software failure, electrical surges and power outages. This section defines additional features of the Colleges computer network that minimize the loss of data in the event of such a disaster. No disaster recovery plan can account for every situation that may arise. Common sense plays an important role in this regard. **The most critical part of disaster recovery is not the physical machine but the data created by the user.** Machines and associated hardware can be replaced assuming availability of funds or spare components on-hand. Data that is lost is lost forever and cannot be replaced unless there is a plan in place to account for recovery of data. This is why it is imperative that students back up their data on external encrypted devices (i.e. flash drive, external hard drive, etc.).

11 - SUMMARY

Due to the myriad of circumstances no single policy document may account for every aspect of computer usage**. These policies and procedures are designed to assist the student in maintaining a consistent degree of productivity in the use of computers as a tool in meeting their needs and responsibilities.** They also serve to minimize financial loss in time and materials to the University. Through compliance, each user reduces the likelihood of data or property loss and contributes to a safe and productive working environment.

Please Note:

Windows XP will no longer be supported by Microsoft starting in April 2014. This means that no security patches will be available after that date and will leave your computer vulnerable to viruses and other attacks. After the end-of-support date, any Windows XP computer will be blocked from the HSC campus network.

12 - APPENDICES

12.1 - Appendix I: Setting Screen Saver Password

Setting Screen Saver Password

12.2 - Appendix II: Accessing Network Files and Folders

Accessing Network Files and Folders

12.3 - Appendix III: Print Services and Wireless Networks

Print Services and Wireless Networks

12.4 - Appendix V: OKC Classroom Technology Resources

OKC Classroom Technology Resources

12.5 - Appendix VI: Quick Reference

Quick Reference