Acceptable Use of Technology Resources
DISPOSAL PROGRAM OVERVIEW ..................................................................................................... 40

IT Access to Offices ......................................................................................................................... 41

PURPOSE .............................................................................................................................................. 41

POLICY ................................................................................................................................................... 41

PROCEDURE ......................................................................................................................................... 41

Access to Network Rooms and IT Storage Areas ............................................................................... 42

PURPOSE .............................................................................................................................................. 42

POLICY ................................................................................................................................................... 42

Requesting IT Assistance .................................................................................................................... 43

POLICY ................................................................................................................................................... 43

EMPLOYEES.......................................................................................................................................... 43

Classroom Technical Assistance: ........................................................................................................ 43

Event Technical Assistance: ................................................................................................................ 43

Other Technical Assistance: ................................................................................................................ 43

STUDENTS ............................................................................................................................................. 43

OTHERS ................................................................................................................................................. 43

Remote Access ................................................................................................................................... 44

PURPOSE .............................................................................................................................................. 44

POLICY ................................................................................................................................................... 44

Equipment Usage ............................................................................................................................... 45

PURPOSE .............................................................................................................................................. 45

EQUIPMENT LENDING AND NEW EQUIPMENT REQUESTS ........................................................... 45

IT EQUIPMENT PURCHASES ............................................................................................................... 45

PERSONAL HARDWARE ..................................................................................................................... 45

SOFTWARE INSTALLATION ................................................................................................................ 45

MAINTENANCE ..................................................................................................................................... 46

EQUIPMENT RELOCATION .................................................................................................................. 46

EMPLOYEE EQUIPMENT RESPONSIBILITIES ................................................................................... 46

BLACKBERRY AND CELL PHONE USAGE ........................................................................................ 46
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff Equipment Distribution</td>
<td>48</td>
</tr>
<tr>
<td><strong>PURPOSE</strong></td>
<td>48</td>
</tr>
<tr>
<td><strong>POLICY</strong></td>
<td>48</td>
</tr>
<tr>
<td><strong>EXCLUSIONS</strong></td>
<td>48</td>
</tr>
<tr>
<td>DESKTOPS</td>
<td>48</td>
</tr>
<tr>
<td>LAPTOPS</td>
<td>48</td>
</tr>
<tr>
<td>MIFI DEVICES</td>
<td>49</td>
</tr>
<tr>
<td>PRINTERS</td>
<td>49</td>
</tr>
<tr>
<td>Faculty Equipment Distribution</td>
<td>50</td>
</tr>
<tr>
<td><strong>PURPOSE</strong></td>
<td>50</td>
</tr>
<tr>
<td><strong>POLICY</strong></td>
<td>50</td>
</tr>
<tr>
<td>DESKTOPS</td>
<td>50</td>
</tr>
<tr>
<td>LAPTOPS</td>
<td>50</td>
</tr>
<tr>
<td>MIFI DEVICES</td>
<td>50</td>
</tr>
<tr>
<td>PRINTERS</td>
<td>51</td>
</tr>
<tr>
<td>Computer Lab Usage</td>
<td>52</td>
</tr>
<tr>
<td><strong>PURPOSE</strong></td>
<td>52</td>
</tr>
<tr>
<td><strong>POLICY</strong></td>
<td>52</td>
</tr>
<tr>
<td><strong>ENFORCEMENT</strong></td>
<td>52</td>
</tr>
<tr>
<td>Computer Classroom Usage</td>
<td>53</td>
</tr>
<tr>
<td><strong>PURPOSE</strong></td>
<td>53</td>
</tr>
<tr>
<td><strong>POLICY</strong></td>
<td>53</td>
</tr>
<tr>
<td>Student Laptop Usage</td>
<td>54</td>
</tr>
<tr>
<td><strong>PURPOSE</strong></td>
<td>54</td>
</tr>
<tr>
<td><strong>POLICY</strong></td>
<td>54</td>
</tr>
<tr>
<td><strong>MONITORING AND ENFORCEMENT</strong></td>
<td>54</td>
</tr>
<tr>
<td>Work Studies, Volunteers, and Interns</td>
<td>56</td>
</tr>
<tr>
<td><strong>PURPOSE</strong></td>
<td>56</td>
</tr>
<tr>
<td><strong>POLICY</strong></td>
<td>56</td>
</tr>
</tbody>
</table>
Student Laptop Lending Program ................................................................. 57
  PURPOSE ........................................................................................................... 57
  POLICY .............................................................................................................. 57
  PROCEDURE ..................................................................................................... 57
Violations ........................................................................................................... 59
  REPORTING VIOLATIONS ............................................................................... 59
  INVESTIGATION ............................................................................................... 59
  PENALTIES ....................................................................................................... 59
*Acceptance ..................................................................................................... 60

RELATED DOCUMENTS .................................................................................. 61
  Academic Honesty Policy ................................................................................ 62
  Email Best Practices ......................................................................................... 62
  Information Assurance Policy .......................................................................... 62
  Student Laptop Lending Request Form .......................................................... 62
  Student Identification Procedure ..................................................................... 62
  Media Duplication and Home/Personal Use Software Installation Request Form .. 63
IT Department Vision, Mission, and Principles

VISION

The Hodges University Department of Information Technology will become a recognized leader in the formulation, development, and implementation of innovative technological solutions in a collegiate environment.

MISSION

The Department of Information Technology’s mission is to guide the selection, procurement, development and implementation of innovative technological enhancements, to ensure a positive user experience, and to provide exemplary customer service for the University community.

MISSION PRINCIPLES

To achieve its mission, the Department of Information Technology supports the following principles:

- To maintain mutually beneficial relationships with vendors, service providers, and University departments.
- To provide superior user support and training.
- To maintain and enforce appropriate security procedures and protocols.
- To sustain and enforce proactive system maintenance that minimizes downtime.
- To provide continuous quality review and improvement of IT systems and processes.
- To provide a work environment that encourages team collaboration, positive attitude, and high morale.
- To maintain appropriate budgetary controls over IT allocated funds.
- To provide appropriate redundancy and failover solutions in order to minimize downtime and facilitate disaster recovery.
Introduction

The following policies supersede all other existing Information Technology policies.

Hodges University provides technology resources to faculty, staff, students and alumni expressly for the purpose of conducting University business in support of the mission and goals of the University.

Users must understand that this access is expressly for the purpose of fulfillment of job responsibilities and not for non-business activities. Users must also understand that any connection to the Internet offers an opportunity for unauthorized users to view or access corporate information. Therefore, it is important that all connections be secure, controlled, and monitored.

To this end, University users should have no expectation of privacy while using University-owned or University-leased equipment or resources. Information passing through or stored on University equipment can and will be monitored. Users should also understand that the University maintains the right to monitor and review Internet use, e-mail communications, or other electronic communications sent or received by users.

Purpose

This document constitutes the University-wide policy intended to allow for the proper use of all Hodges University network, communications, and information resources, effective protection of individual users and their personal information, equitable access, and proper management of those resources as well as procurement, inventorying, and maintenance of equipment. This policy applies to both internal and external access to Hodges University technology resources.

Access to technology resources owned or operated by Hodges University imposes certain responsibilities and obligations, and is granted subject to University policies and local, state and federal laws. Appropriate use should always be legal, ethical, reflect academic honesty, reflect University standards and show restraint in the consumption of shared resources.

Authority

The following policies have full support from the Hodges University administration. The Information Technology (IT) department administers these policies, which are currently effective for all University employees and resources. Full cooperation with this policy is required so that all goals can be met in accordance with the University Mission.

Continuance

The University may modify these policies at any time. Users should review University policies on a regular basis.
Scope

These policies apply to all employees, contractors, consultants, temporaries, work studies, guests and other users of University resources.

Definitions

**Authorized Users**: Authorized users are (1) current faculty, staff and students of Hodges University; (2) others whose access furthers the mission of the University and whose usage does not interfere with faculty, staff and student access to resources.

**Authorized Use**: Authorized use of Hodges University owned or operated Internet, network, email, and other technology resources refers to all use that is consistent with the education, research, and mission of this University and these policies.

**Resources/Technology Resources**: The terms Resources and Technology Resources are used herein to refer to all network, communications (IM, email, phone), and Internet access provided by the University as well as all technology equipment and any software application and its data, that are licensed by or considered the property of the University.

**Employee**: Full or part-time faculty or staff employed by Hodges University. In this context employee may also include tutors, work study students, temporary workers and consultants.
Administrative Rights and Privileges

Allocation of Resources
Hodges University reserves the right to allocate resources in any way that supports its overall mission.

See “Equipment Policies”

Enforcement and Imposition of Sanctions
Hodges University has the right to enforce all policies contained herein and may impose sanctions and penalties on anyone who violates these usage policies up to and including termination and legal action. Individual access may be suspended for reasons deemed relevant by these policies and University administration.

See “Violations”

Investigation
Hodges University has the right to investigate any suspected misuse of technology resources employing any and all methods available.

See “Investigation” section of “Violations”

Administrative Access
IT Staff members may access others’ files for the maintenance and administration of technology resources, such as to create backup copies of media. However, in all cases, individuals' privileges and rights of privacy will be respected to the greatest extent possible.

See “User Privacy”

Monitoring
The Information Technology Department of Hodges University, while managing the operation of computers and networks, may routinely monitor and log usage data. These persons may review this data to ensure appropriate resource allocation and utilization, for evidence of violation of law or policy, and other purposes.

With authorization, the Director of IT may monitor the activities of and inspect the files of users. University officials reserve the right to access and examine the files and/or actual network activity of any user to investigate violations or suspected violations of security and/or policies. For this reason, users must regard themselves as having no expectation of privacy with regard to their files, electronic activities, data or communications.

See “User Privacy”

Security Procedures
Hodges University has the right to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional information, however stored, and to impose appropriate penalties when security is breached by negligence or intent.

See Information Assurance Policies
Permitted Use of Resources

University technology resources are primarily for authorized business use by authorized users. Occasional and reasonable personal use is permitted, provided that this does not interfere with the performance of work, academic duties, or other related responsibilities of any user. Authorized users may use University Internet services for personal improvement, outside of scheduled hours of work, provided that such use is consistent with professional conduct and is not for personal financial gain. Note - it is expected that certain resources, such as Internet and email, provided by Hodges University will be used for University business but with the understanding that some personal use may take place if done so in a reasonable and judicious manner in accordance with current policies.

Resources at Hodges University are provided strictly in support of University activities. In open access areas if a computer is needed for class-related work, a user who is not performing class-related work must relinquish the workstation upon request.

Prohibited Use of Resources

The use of computing facilities not open for public use, the use of closed facilities not assigned for instruction, or the use of resources not directly assigned to the individual without authorization violates usage policies and may subject the offender to sanctions.

Harmful Activities: Activities that are harmful to University resources are prohibited. These include, but are not limited to, creating or propagating viruses, disrupting services, damaging files, intentional destruction of or damage to equipment, software, or data belonging to Hodges University or other users. Reasonable and judicious use should be made of all technology resources. Frivolous and/or unnecessarily large or lengthy transmissions should be avoided. Streaming audio/video that does not have educational merit is prohibited. See “Streaming Media.”

Users shall not use University resources to view, play, participate in, download, save, receive, or send material (e.g. music, photo or video files) that is not related to academic or business purposes. Users must not deliberately perform these or other actions that waste limited resources or monopolize them to the exclusion of others.
The following are strictly prohibited:

- Viewing of offensive or inappropriate content of any kind, including pornographic material.
- Promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability.
- Messages of a religious, political, or racial nature.
- Game playing, gambling, streaming personal music, video or other audio files and peer-to-peer file sharing. See "Peer-to-Peer and File Sharing" and "Streaming Media".
- Threatening or violent behavior.
- Illegal activities.
- Personal financial gain or other unauthorized commercial enterprise.
- Solicitation for activities/services not directly related to the Hodges University business or authorized activities are prohibited.
- Forwarding e-mail chain letters, phishing, virus, spyware or other harmful content.
- Spamming, spoofing, or illegally accessing resources using University e-mail accounts or equipment.
- Sharing material protected under copyright laws.
- Sending unprotected business-sensitive information by e-mail or over the Internet.
- Dispersing corporate data to unauthorized parties without authorization.
- Facilitating unauthorized access to any University resource.
- Accessing, copying, alteration, or destruction of another users personal files without explicit permission, authorization or if required to do so by law, warrant or regulation. Simply being able to access a file or other information does not imply permission to do so. Such action is still prohibited.
- Storing passwords or other information that can be used to gain access to campus resources in plain sight. Such information should be stored in a secure environment. Login accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. You are responsible for any unauthorized use of your account. See "Password Policy".
- The use of technology resources for purposes that involve academic dishonesty is a violation of University policy. See Academic Honesty Policy.

System Abuse

All personnel are responsible for their actions. If accidents happen, immediately notify the IT department. Damage will be evaluated, if any. If negligence was involved in the loss or extensive repair is needed to computer equipment, the user responsible may be required to pay for damages and prohibited from further access to University resources.

Deliberate attempts, such as denial of service attacks, intended to degrade the performance of a system or network, to deprive authorized personnel or other constituents of resources or access to any University technology resource, or to gain unauthorized access to resources are prohibited.

Harassment

Rules of conduct of the University related to any form of harassment apply to the use of technology resources. Abusive behaviors are not permitted. Abusive behaviors include the utilization of resources to harass others in some way; for instance, sending electronic messages that are abusive, obscene, threatening or a nuisance. Obscene, vulgar, or derogatory output prominently displayed on a public workstation or printed and left out in public areas is prohibited. No member of Hodges University (staff, faculty, student or guest) is permitted to use University technology resources to view, save, print, send or any function involving lewd, pornographic, obscene or vulgar material of any kind. Complaints of behavior that appears to constitute misuse of resources will result in an investigation by University officials, and appropriate action will be initiated. Behavior involving pornography will result in immediate dismissal from the University.
Responsibilities

Access to University resources is a privilege provided in order to conduct the business of the University. However, it must be understood that privileges are conditioned upon acceptance of the accompanying responsibilities.

Authorized users must:

- Honor acceptable use and other University policies.
- Abide by existing federal, state, and local privacy, telecommunications, networking, and other applicable laws and regulations.
- Abide by copyright laws.
- Minimize unnecessary network traffic (i.e. streaming media) that may overload networks, waste resources and interfere with the ability of others to make effective use of network resources.
- Refrain from malicious or unauthorized transmissions or monitoring.
- Similarly, no one should connect to a remote computer on the network without prior written permission from the administrator of that system unless given legally justifiable cause to do so.
- You are responsible, in coordination with the Information Technology Department, for the security and integrity of University information stored on your University assigned system.
- Control physical and network access to the machine, and not disable virus protection, anti-spyware or other software required by the University.
- Strictly control confidential access information.

Unauthorized Access

Unauthorized access to resources is prohibited. In particular, users are not permitted to engage in activities that are detrimental to the system or other users. These include, but are not limited to: damaging computer systems, obtaining access to resources not authorized to you, depriving another user of authorized resources, and gaining unauthorized access to systems.

Examples of prohibited means of obtaining unauthorized access include, but are not limited to; hacking, the use of key loggers or other software designed to capture secure information, using privileges granted during a previous position at the University, unauthorized physical access and any other unauthorized access to electronic files. The use of any computer program or device to intercept or decode passwords or similar access control information is prohibited.

You may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users. Such action may result in dismissal and may incur legal action.

You may not allow unauthorized use of University resources by family, friends, etc. Use of computers and other resources by siblings, children, spouses or other family and friends constitutes a security risk and is strictly prohibited.

Use of Privileged Access

Special access to information or other special privilege is to be used in performance of official duties only. Information that you obtain through special privileges is to be treated as confidential. No information categorized as confidential, sensitive or proprietary shall be stored on unapproved removable media, such as CD, DVD, ZIP, unencrypted media, or unauthorized mobile devices such as personal devices. Confidential, sensitive or proprietary information also should not be emailed to personal email addresses. In addition, external storage of student, faculty and/or staff's personal, private or financial information,
including student grades, is prohibited. A network user share and VPN access is provided for employees so local back-ups or back-ups on removable media is not necessary. Network shares are backed up regularly by the IT department and may be restored on request.

See “Data Backup and Restoration Policy”

See Portable Media Policies section of Information Assurance Policy

**Termination and Review of Individual Access**

When you cease being an authorized user, IT will be notified and access to University resources will be immediately terminated. If you are assigned a new position and/or responsibilities within the University, your access authorization must be reviewed. You will not be granted access to facilities, accounts, access codes, privileges, or information for which you are not authorized in your new circumstances.

Users leaving employment with the University are responsible for ensuring that they have relinquished any Hodges University owned equipment, access information, and keys.

**Account Audits**

The Department of Information Technology regularly reviews all network and application access.

See Information Assurance Policy

**User Privacy**

The University will preserve the individual's privacy to the greatest extent possible, while reserving the right to monitor system usage. Electronic and other technological methods must not be used to infringe upon privacy unless there is a specific cause to do so. Users, however, utilize University resources at their own risk.

See “Administrative Rights and Privileges”
Copyright, Intellectual Property, and Software Use

PURPOSE

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Users must pre-suppose that all materials on the Internet are copyrighted unless specifically stated otherwise. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the University community.

Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software may be a violation of federal and state law.

POLICY

You are responsible for recognizing and honoring the intellectual property rights of others. Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to all works of all authors and publishers in all media. It encompasses the right to acknowledgements, right to privacy, and right to determine the form, manner, and terms of publication.

Any intellectual material created using University licensed software by an employee of Hodges University or while acting as an employee of the University is to be the property of Hodges University.

1) According to U.S. Copyright Law, using, inspecting, copying and storing copyrighted computer programs and other material, in violation of copyright, is prohibited. Persons involved in illegal reproduction of the software or related documentation can be subject to civil damages of as much as $50,000, and criminal penalties, including fines and imprisonment. Hodges University does not condone the illegal duplication of software or related documentation.

2) Hodges University licenses the use of computer software from a variety of outside companies. Hodges University does not own this software or its related documentation, and users, unless specifically authorized by the software developer; do not have the right to reproduce or share it.

3) Hodges University students and employees learning of any misuse of software or related documentation within the University shall notify the Director of Information Technology or a supervisor. Failure to report misuse may result in disciplinary action that could include termination of your relationship with Hodges University.

4) File sharing or peer to peer applications used to illegally share music, videos, or other copyrighted information are prohibited. See “Peer to Peer and File Sharing”

Hodges University students or employees, who make, acquire or use unauthorized copies of computer software, its related documentation, or other copyrighted information shall be disciplined as appropriate under the circumstances.

See “Violations”
MEDIA DUPLICATION REQUESTS

Any request for media duplication submitted to IT must be accompanied by a Media Duplication Request form. It is up to the requestor to fill out the form and provide appropriate documentation of permission of Copyright owner.

USE OF LICENSED SOFTWARE

No software may be installed, copied, or used on University resources except as permitted by the owner of the software. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to. NO SOFTWARE IS TO BE INSTALLED BY ANYONE OTHER THAN THE INFORMATION TECHNOLOGY STAFF.

See “Software Installation”
Peer-to-Peer and File Sharing

PURPOSE

H.R 4137, the Higher Education Opportunity Act (HEOA), a reauthorization of the Higher Education Act, includes provisions that are designed to reduce the illegal uploading and downloading of copyrighted works through peer-to-peer (P2P) file sharing including:

- Institutions make an annual disclosure that informs students that the illegal distribution of copyrighted materials may subject them to criminal and civil penalties and describes the steps that institutions will take to detect and punish illegal distribution of copyrighted materials.
- Institutions certify to the Secretary of Education that they have developed plans to “effectively combat” the unauthorized distribution of copyrighted material.
- Institutions, “to the extent practicable,” offer alternatives to illegal file sharing.
- Institutions identify procedures for periodically reviewing the effectiveness of the plans to combat the unauthorized distribution of copyrighted materials.

Peer-to-peer and file sharing applications allow sharing of files amongst participating users. Sharing audio, video, data, or anything in digital format is common and may be in violation of copyright. In accordance with the HEOA Hodges University uses web filtering technologies to actively block P2P file-sharing applications.

POLICY

This policy is meant to prohibit the use of Peer-to-Peer (P2P) file-sharing applications for the following reasons:

- Realize the maximum productivity from each employee.
- Address any potential liability from instances when employees download copyrighted material.
- Minimize network disruption.
- Protect the network from exposure to malicious code (worm, virus, Trojan horse).
- Protect the intellectual property of the University and other’s intellectual property.

LIABILITY

Although many materials have been placed on P2P networks with a creator’s consent, much of the material (images, software, movies, music, and video) has been duplicated from copyrighted materials. Downloading such files onto or using University resources places the University at significant risk for legal action by the copyright holder and other organizations. File-sharing networks also provide ready access to inappropriate or offensive material, subjecting the University and its employees to additional legal risk.

DISRUPTION OF SERVICES

While the University has significant Internet bandwidth to accommodate all business-related activity, performance can degrade significantly when P2P file-sharing applications are used, especially when large files are being downloaded. This problem is compounded when other users on the P2P network use University bandwidth to download files from the employee’s computer, which can significantly slow other services such as e-mail, Web browsing, and—more significantly—University website, portal and student applications.
SECURITY

P2P networks can introduce significant gaps in an otherwise secure network. Threats such as worms and viruses can easily be introduced into the University network. P2P applications, if modified, can also allow users outside the University to gain access to data on the employee’s computer or even the corporate network. Although most P2P applications allow users to disable file-sharing, such measures do little to prevent threats from being downloaded onto a user’s machine. Some P2P applications will also allow third parties to see the user’s IP address. The use of so-called spyware, which can allow network users to see your Internet browsing or can harness the use of your machine’s resources, is also common on many P2P applications. P2P applications could also disrupt software on an employee’s workstation.

PRIVACY

The use of P2P file-sharing applications can sometimes allow other members of the P2P network to have access to resources on your local machine, putting the University’s data and information assets, as well as an employee’s personal information, at risk.
Streaming Media

PURPOSE

While there are many legitimate business and academic applications that use streamed audio and video, some streaming media content is strictly entertainment-based and serves no enterprise value. Streaming media may consume significant network bandwidth and can delay access to and/or prevent other users from accessing resources and completing critical tasks.

POLICY

University computer systems and network must be used only for business or academic activities. Legitimate streaming media use, such as when streaming media applications and files are employed to conduct research, view financial and media reports, or complete University-sponsored training programs, constitutes acceptable use. Incidental personal use of University resources for the purpose of streaming media is not permissible. The use of University resources, including computer, server, and network use, should never create either the appearance or the reality of inappropriate use.

Streaming audio/video that does not have educational or business merit is prohibited.
Third Party Service Providers

PURPOSE

The University frequently outsources projects and technical assistance to third party providers. This policy is to protect the University, its constituents, services and data as well as its relationship with providers.

POLICY

Hodges IT Department strives to ensure that all contracts with third party service providers include a confidentiality clause. In the event that the original service contract or license agreement between Hodges University and the third party does not have a confidentiality section that meets the requirements of access to University resources, a signed Hodges University Confidentiality Agreement (see Information Assurance Policy) must be on file with the IT Department before any access may be granted.

Consultants, service providers, and other contracted third parties will be granted access to University systems and/or information on a 'need to know' basis. If a third party requires a network account, IT must be notified and must validate the need for access. IT will also require information with regard to the specific areas of access required. IT may deny the third party access if unable to validate the need. Third party users/vendors are responsible for the security of their password(s) and accountable for any activity resulting from the use of their user ID(s) within reasonable scope of their control. Hodges University will terminate access for any third party in the event of misuse of access or termination of contract.

Third parties shall implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the confidentiality, integrity, and availability of all electronically managed information. Upon termination of services, third parties will also return all information or certify destruction of information according to the agreement and/or specific terms of the contract. Third party providers are also responsible for protection of account and password(s) and any other protection the account has, as well as reporting suspected misuse or information security incidents according to the reporting procedure established by the current Information Assurance Policy. In the event of an information security incident caused by a third party provider, the third party may be held legally liable for damages and expenses related to recovery/disclosure activities, punitive damages, and legal expenses incurred by the University.
Student Usage of Electronic Communication Resources

Hodges University email will be used as the primary form of communication with students. Applications like Blackboard and student email provide forums for academic discourse. These policies apply to all electronic communications systems supplied by the University. This includes but is not limited to:

- Blackboard and associated Blackboard tools (e.g. discussion boards, audio, video, and chat) and
- University email.

PURPOSE

Hodges University provides electronic mail, Blackboard, Blackboard tools, and other electronic communication services to students as well as various communication resources for alumni. The purpose of this policy is to provide the following information:

1. Inform students about the applicability of law and University policy concerning electronic mail and other communication resources;
2. Provide guidelines for use of electronic mail, Blackboard and other communication resources at Hodges University;
3. Give specific examples of prohibited activities involving electronic communications; and
4. Inform students about specific issues of privacy, authenticity and risk related to e-mail and other electronic communications.
5. Provide guidelines for behavior involving electronic communications.

University Student Behavior Standards, Academic Honesty Policy and other applicable policies also apply.

POLICIES:

When using Hodges communication resources applications you should:

- Respect other people's views and beliefs.
- Post comments appropriate to the particular discussion.
- Enjoy your interaction with fellow students, faculty and others in a friendly and intellectually stimulating environment.
- Maintain academic integrity.

ACCEPTABLE USE OF BLACKBOARD

The University uses several modes of electronic communications such as the Blackboard learning management system (LMS). Blackboard does not only contain learning and teaching materials and links to outside resources, it is also a communication system. These communication capabilities include email function, discussion boards, chat, voice boards, and other asynchronous and synchronous communication tools.

Many of these communications and discussions are taking place in a social environment. Normal rules of social interaction apply and the remoteness of the recipients must not be used as an excuse to behave in an anti-social or inappropriate manner.
Examples of prohibited behavior are:

- Inappropriate or impolite behavior or language.
- Transmission or linking of offensive, hostile or inappropriate content of any kind, including pornographic material.
- Promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability.
- Messages of a religious, political, or racial nature.
- Threatening, demeaning, aggressive or violent behavior or content.
- Messages promoting personal financial gain or other unauthorized commercial enterprise.
- Solicitation for activities/services not directly related to Hodges University business or that are unauthorized are prohibited.
- Forwarding e-mail chain letters, phishing, virus, spyware or other harmful content.
- Sharing material protected under copyright laws.
- Transmitting business-sensitive information to unauthorized parties.
- The use of technology resources for purposes that involve academic dishonesty is a violation of University policy. See the Academic Honesty Policy.
- Personal comments about other students and their views.

See “Prohibited Use”

ACCEPTABLE USE OF EMAIL

Hodges University encourages the use of e-mail in support of instruction, research and public service. Students are urged to make extensive use of e-mail to communicate with their instructors, support staff and fellow students. Students are expected to use e-mail services responsibly and to comply with all applicable local, state and federal laws, and University policies.

LIMITS

Because student email is outsourced to Microsoft’s cloud email service, Hodges University does not currently set attachment, mailbox size, or other limits on student email. The University reserves the right to change this policy at any time.

SPECIFIC PROHIBITIONS

It is not possible to provide a comprehensive list of all possible violations. However, the following is a list of activities specifically prohibited:

- Use of e-mail to threaten or harass individuals on or off campus. Offensive messages (i.e. messages with sexual, discriminatory, racial or derogatory connotations) are prohibited and will be considered harassment. Harassment in any form is prohibited.

- Use of a false e-mail addresses (i.e. mail "spoofing"). Deliberately sending mail with a misleading or false e-mail address is prohibited. Forgery, or attempted forgery, of the "From:" line in an e-mail message is prohibited. Masking the identity of an account and/or electronic address is prohibited.

- Any attempt to disrupt another person’s ability to use his/her accounts. Examples include sending excessive or repetitious e-mail; attempts to contact another user via e-mail, telephone or in person, after being told that such contact is not desired. Violation of such a request will be considered harassment and is prohibited.
The sending of excessively large quantities of e-mail. An excessively large quantity of mail may be defined as a small message sent to a very large number of users, a very large message sent to several users, or anywhere in between.

Sending unsolicited commercial or bulk e-mail, including advertisements, is prohibited. Examples include sending mass mailings to advertise a product or service. Note that this prohibition extends to “spamming”, i.e. sending solicitations to many users, newsgroups or others without express consent on the receiver’s behalf.

The sending of any material that contains viruses and/or other harmful or malicious programs.

The initiating or forwarding of “chain letters”. A chain letter is an e-mail message whose primary purpose is to propagate itself indefinitely. Chain letters waste employee time and network resources, slowing mail delivery and other network services. Note also that chain letters are “illegal if they request money or other items of value and promise a substantial return to participants” (U.S. Postal Inspection Service).

Violation of privacy. Monitoring or attempting to monitor other people’s communications without their permission or knowledge. Users should not view, read, listen to, copy, change, execute or delete another user’s information without that user’s or the owner’s permission.

Attempts to gain unauthorized access to the services or other accounts through password mining, phishing or any other means. Security measures are in place to protect the privacy of Hodges University users. Any attempt to bypass these security measures, or to secure a higher level of access or privilege without appropriate authorization, is prohibited.

Use of services for commercial purposes. Users may not sell or otherwise provide access to their account or perform work for profit in a manner not authorized by Hodges University.

Hodges University student e-mail cannot be used to upload/download copyrighted materials, trade secrets, proprietary financial information or similar materials without the appropriate prior authorization from the intellectual property owner.

ACCOUNT REMOVAL/TERMINATION

Again, because student email is outsourced to Microsoft’s live@edu cloud service, Hodges University does not currently have an account removal policy related to account inactivity. Hodges University reserves the right to remove any student or alumni accounts due to inappropriate activity and/or policy violation. Removal of accounts for students who have a “withdrawn” or “cancelled on enrollment” status is up to the discretion of Hodges University and will be handled on a case by case basis.

RESPONSIBILITIES

Access to technology resources owned or operated by Hodges University imposes certain responsibilities and obligations and is granted subject to these University policies and local, state and federal laws. Appropriate use should always be legal, ethical, reflect academic honesty, reflect University standards and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property; ownership of data; system security mechanisms and individual rights to privacy and freedom from intimidation, harassment and unwarranted annoyance. Appropriate use of University resources includes instruction; independent study; authorized research; independent research; communications; and official work of the offices, units, recognized student and campus organizations and agencies of the University.
COPYRIGHT

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

VIOLATION

If there is reason to believe that an e-mail account is being used in a violation of law or University policy, or if an account is used in a way that threatens to disrupt service to other users, the Department of Information Technology may restrict, suspend or disable that account’s access to e-mail services, until the University is assured that the illegal or disruptive use of the account will cease. Penalties for violation range from account termination and dismissal up to and including legal action.

PRIVACY

University officials reserve the right to access and examine the files and/or actual network activity of any user to investigate violations or suspected violations of security and/or policies. For this reason, users must regard themselves as having no expectation of privacy with regard to their file, electronic activities, data or communications.

RISK AND LIABILITY

There is no guarantee that e-mail is authentic, it is therefore prudent to be skeptical of the “From:” addresses that appear in messages. Mail between campuses or from off-campus sites can be very easily “spoofed”, i.e. the message is sent in such a way that it appears to be from a different sender than it truly is. Anyone who has doubts about the identity of the sender of any message should communicate with the purported sender by some other means to confirm the content of the message.

It is the user’s responsibility to employ appropriate risk mitigation techniques and to be aware of current threats such as phishing, spam, viruses, etc.

Hodges University assumes no liability for any damages that are incurred while using University email services.

See Email Best Practices
Employee Email Usage

The University encourages all employees to use their Hodges University email addresses as their primary means of communication, while conducting business that in any way represents Hodges University.

PURPOSE

Hodges University provides electronic mail services to employees. The purpose of this policy is to provide the following information:

1. Inform employees about the applicability of law and University policy concerning electronic mail;
2. Provide guidelines for use of electronic mail at Hodges University;
3. Give specific examples of prohibited activities involving electronic mail; and
4. Inform employees about specific issues of privacy, authenticity and risk related to e-mail.

POLICIES:

ACCEPTABLE USE OF EMAIL

Hodges University encourages the use of e-mail in support of Hodges related business activities, instruction, research and public service. Faculty are urged to make extensive use of e-mail to communicate with students. Users are expected to use e-mail services responsibly and to comply with all applicable local, state and federal laws, and University policies.

LIMITS

In order to control storage requirements and to ensure availability and equitable access to Hodges University email services, the Information Technology department sets limits on mailbox size and email attachment size.

Attachments: Authorized users may send and receive e-mail attachments that do not exceed the established limit of 10MB. All attachments are scanned by University antivirus software.

Mailbox Size: Employee mailbox size is limited based on the user’s position at the institution. Users are alerted when the mailbox size approaches these limits. Should the user reach this limit and take no further action, they will not be able to send or receive email until the mailbox size is addressed. It is recommended that users consistently and regularly review, delete, and/or archive their email to control mailbox size.

ACCOUNT REMOVAL/TERMINATION

Employees: Upon notification of employee termination, email access will be immediately terminated. Access to an employee’s email may be requested by a supervisor to ensure that customer service needs are met without interruption.

RESPONSIBILITIES

Access to technology resources owned or operated by Hodges University imposes certain responsibilities and obligations and is granted subject to these University policies and local, state and federal laws.
Appropriate use should always be legal, ethical, reflect academic honesty, reflect University standards and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property; ownership of data; system security mechanisms and individual rights to privacy and freedom from intimidation, harassment and unwarranted annoyance. Appropriate use of University resources includes instruction; independent study; authorized research; independent research-communications; and official work of the offices, units, recognized student and campus organizations and agencies of the University.

COPYRIGHT

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

VIOLATION

If there is reason to believe that an e-mail account is being used in a violation of law or University policy, or if an account is used in a way that threatens to disrupt service to other users, the Department of Information Technology may restrict, suspend or disable that account’s access to e-mail services, until the University is assured that the illegal or disruptive use of the account will cease. Penalties for violation range from account termination and dismissal up to and including legal action.

SPECIFIC PROHIBITIONS

It is not possible to provide a comprehensive list of all possible violations. However, the following list of activities is specifically prohibited:

- Use of e-mail to threaten or harass individuals on or off campus. Offensive messages (i.e. messages with sexual, discriminatory, racial or derogatory connotations) are prohibited and will be considered harassment. Harassment in any form is prohibited.

- Use of a false e-mail addresses (i.e. mail "spoofing"). Deliberately sending mail with a misleading or false e-mail address is prohibited. Forgery, or attempted forgery, of the “From:" line in an e-mail message is prohibited. Masking the identity of an account and/or electronic address is prohibited.

- Any attempt to disrupt another person’s ability to use his/her accounts. Examples include sending excessive or repetitious e-mail; attempts to contact another user via e-mail, telephone or in person, after being told that such contact is not desired. Violation of such a request will be considered harassment and is prohibited.

- The sending of excessively large quantities of e-mail. An excessively large quantity of mail may be defined as a small message sent to a very large number of users, a very large message sent to several users, or anywhere in between.

- Sending unsolicited commercial or bulk e-mail, including advertisements, is prohibited. Examples include sending mass mailings to advertise a product or service. Note that this prohibition extends to “spamming”, i.e. sending solicitations to many users, newsgroups or others without express consent on the receiver’s behalf.

- The sending of any material that contains viruses, other harmful or malicious programs.
The initiating or forwarding of “chain letters”. A chain letter is an e-mail message whose primary purpose is to propagate itself indefinitely. Chain letters waste network resources, slowing mail delivery and other network services. Note also that chain letters are “illegal if they request money or other items of value and promise a substantial return to participants” (U.S. Postal Inspection Service).

Violation of privacy. Monitoring or attempting to monitor other people’s communications without their permission or knowledge. Users should not view, read, listen to, copy, change, execute or delete another user’s information without that user’s or the owner’s permission.

Attempts to gain unauthorized access to the services or other accounts through password mining, phishing or any other means. Security measures are in place to protect the privacy of Hodges University users. Any attempt to bypass these security measures, or to secure a higher level of access or privilege without appropriate authorization, is prohibited.

Use of services for commercial purposes. Users may not sell access to their account or perform work for profit in a manner not authorized by Hodges University.

Hodges University e-mail cannot be used to upload/download copyrighted materials, trade secrets, proprietary financial information or similar materials without the appropriate prior authorization from the intellectual property owner.

PRIVACY

University officials reserve the right to access and examine the files and/or actual network activity of any user to investigate violations or suspected violations of security and/or policies. For this reason, users must regard themselves as having no expectation of privacy with regard to their file, electronic activities, data or communications.

RISK AND LIABILITY

There is no guarantee that e-mail is authentic, it is therefore prudent to be skeptical of the “From:” addresses that appear in messages. Mail between campuses or from off-campus sites can be very easily “spoofed”, i.e. the message is sent in such a way that it appears to be from a different sender than it truly is. Anyone who has doubts about the identity of the sender of any message should communicate with the purported sender by some other means to confirm the content of the message.

It is the user’s responsibility to employ appropriate risk mitigation techniques and to be aware of current threats such as phishing, spam, viruses, etc.

Hodges University assumes no liability for any damages that are incurred while using University email services.

See “Virus/Spyware Protection”

See Email Best Practices
Email Formatting and Signature Policy

PURPOSE

Because emails and email signatures contribute to the University and its employees’ professional image, the following email formatting and signature standards are expected of all employees at Hodges University in electronic communications using the University’s electronic communication resources. These standards apply to email messages involving official University communication between employees, students, faculty or other constituents and are not application specific. These standards do not apply to Blackberry or other mobile devices.

Although these standards apply to all official University electronic communications, of primary concern is external communications with business partners, vendors, alumni, students, and the community. In these cases the email signature can be a tool to project a positive image, and various branding/marketing messages for the University.

RESPONSIBILITY

Supervisors are responsible for compliance of their department.

DEFINITIONS

Email Signature: For the purposes of these standards, an “email signature” is defined as any block of text, images or other content that is automatically attached to the end of a message as a means of providing additional information about the University and/or sender of the email.

Official University Communications: Official University electronic communications are defined as any communication of University business between University representatives via electronic mail. This includes employees and some consultants. This does not necessarily include communications between Hodges employees.

POLICY

Signature: All official University e-mail communications should include an email signature at the end of the body of the sender’s email. Each signature is expected to conform to the following professional format and content standards, no additional elements are allowed.

Line 1
First and last name and academic achievement (Ph.D., DBA, Ed. D., JD, MSW, MS, MA, etc. any professional licenses or top level certifications are optional – CPA, CFP etc.) with appropriate punctuation. Check faculty listing in our Catalog or Bulletin for proper punctuation. Middle initial is optional. No prefixes are necessary.

- Example: John L. Doe, DBA
Hodges University Acceptable Use of Technology Resources Policies
Last Revision 8/27/15 mg

---

**Line 2**
- Job Title/Academic Rank and School/Department if not already obvious based on title. No assigned duties or responsibilities should appear in the signature line. Example: do not include "Chair of XXX Committee".
  - Example 1: Director of Information Technology
  - Example 2: Assistant Professor, School of Allied Health
  - Example 3: Systems Engineer/Analyst, Information Technology
  - Example 4: Program Chair, Business Administration

**Line 3**
- Hodges University | the address of your main office location. If you are a remote employee please use the address of the campus where your supervisor is based or the address of the Learning Site where you receive University communications.
  - City should never be abbreviated. Use Naples, Fort Myers, etc.
  - State should be a two letter abbreviation in all CAPS with no punctuation. Example: FL
  - The only acceptable abbreviations in addresses are street designations such as: St., Dr., Blvd., etc.
  - Never abbreviate Suite.

**Line 4**
- Contact information: 1) direct phone line; 2) 800 number; 3) f.-fax if you want to provide it; 4) c.-cell if you want to provide it. Minimally, you should provide an 800 number for your preferred campus. Please note that the examples below are separated by a “pipe” symbol (|), not a slash (/). The pipe symbol is typically located above the “backslash” symbol above the enter key.
  - Example 1: (239) 598-6160 | (800) 466-8017 | f. (239) 598-6261 | c. (239) 287-8628
  - Example 2: (239) 598-6160 | (800) 466-8017 | f. (239) 598-6261
  - Example 3: (239) 598-6160 | (800) 466-8017
  - Example 4: (800) 466-8017

**Line 5**
- Email address and web address. Always use your hodges.edu address NOT your personal email address.
  - Example: asmith@hodges.edu | www.hodges.edu

**Line 6**
- May be used for marketing event graphics and/or taglines approved by administration and marketing department.
- DO NOT USE QUOTES or personal tag lines.
A 5 line staff email signature may look like this:

Amy Smith, Ph.D.
Director of Information Technology
Hodges University | 2655 Northbrooke Drive, Naples, FL 34119
(239) 598-6321 | (800) 466-8017
asmith@hodges.edu | www.hodges.edu

A 5 line faculty email signature may look like this:

Amy Smith, JD
Adjunct Professor, Criminal Justice
Hodges University | 4501 Colonial Blvd., Fort Myers, FL 34119
(239) 598-6321 | (800) 466-8017 | c. (239) 287-1234
asmith@hodges.edu | www.hodges.edu

Signature Options: Where no phone numbers are applicable, the email address and website may be moved up a line. A shorter email signature may be created and used for replies and forwarded messages as long as it has adequate contact information including your name and either a phone number (10 digit formatting as above) or email address.

Email Formatting: Backgrounds and Font Types are important components that may detract from the professionalism and ease of reading for electronic communications. Because of the importance of these elements the University has adopted the following standards:

- **Background/Stationery:** A plain white background with no stationery is the only acceptable format for any official University electronic mail communications.
- **Font Types:** As it is widely accepted that sans-serif fonts are the easiest to read electronically, these are the only font types are approved for email. Examples include: Arial, Helvetica, Calibri, etc. Outlook defaults to Calibri for the email Body. It is best to simply use the default.
- **Font Sizes:** A font size of between 11 and 14 is generally accepted as readable. 11 is the Outlook default, again, it is best to simply use the default.
- **Font Colors:** Use a plain black font in original emails. Colors such as red, blue or green may be used to call out responses or changes in an original email as a reply as well as the reply itself. Light colors such as yellow should be avoided. Outlook defaults to blue for replies.
- **Font Weight:** Do not type emails in all bold type. Only use bold as headings or to call out specific ideas or items.
- **CAPS:** It is generally felt that an email typed in all CAPS is the digital equivalent of screaming. Therefore, it is recommended that emails be typed using proper capitalization.
Instant Messaging

Non-University hosted Instant messaging (IM) systems introduce a serious security risk often exploited by hackers. External IM programs can introduce viruses and Trojan programs that aid hackers’ attempts to illegally obtain sensitive and confidential data. Protecting University resources from unauthorized access is of paramount importance. Adherence to the following IM guidelines plays a critical role in the process.

PURPOSE

This policy’s purpose is to ensure every employee user understands, and agrees to abide by, specific guidelines for using IM services on University-provided computers, systems and networks.

SCOPE

The University’s Instant Messaging Policy applies to all users that operate University-owned computers, access University-provided Internet services or access University-provided electronic or instant messaging services. All users must conform to the guidelines presented in this policy.

POLICIES:

IM APPLICATIONS AND INSTALLATION

The University’s Information Technology Department approves the use of select University hosted IM application – Microsoft Communicator for employee collaboration and Blackboard IM for student collaboration. Some University approved applications (i.e. Blackboard) may have a built-in chat capability. Use of these applications is authorized. The Information Technology Department will install the approved instant messaging application on University systems, at the request of departmental supervisors only. The installation and use of any unauthorized Instant Messaging application is prohibited. Employees and other users must obtain supervisor approval prior to requesting that Microsoft Communicator be installed. Use of other IM software, including, but not limited to; Yahoo, Facebook, Instant Messenger, AOL, and MS Messenger, on any University-provided equipment or systems is strictly prohibited.

ACCEPTABLE USE OF INSTANT MESSAGING

The University provides approved University hosted instant messaging applications as a means of increasing productivity, enabling electronic communications and transacting University business amongst a geographically diverse population. Instant messaging applications and services are provided as required to University employees, and other authorized agents only for the performance and fulfillment of job responsibilities. Instant messaging services are neither provided nor supported for non-business activities; the University’s instant messaging systems are not to be used for personal activities and no University business is to be conducted on other IM systems.

MONITORING

Instant messaging transactions may contain University information, including proprietary, sensitive and confidential data. In order to properly audit and secure its network, systems, computers and data, IT may monitor instant messaging use; the University may, at its discretion and without notice, monitor use of our instant messaging service at any time. Information and instant message communications passing through or stored on University equipment can and may be monitored and may be archived for storage. Users should have no expectation of privacy when using University-owned, University-leased or University-provided messaging services.
OWNERSHIP

All instant messages, including backup and archive copies, sent or received using University-provided systems become the property of the University. Instant messages sent or received using University-provided accounts or systems are not the property of users. If requested, staff, faculty and others must surrender all IM-related material to the University in a timely manner and the University-based IM account may be terminated without notice.
Virus/Spyware Protection

PURPOSE

It is the responsibility of each user of University resources to take reasonable measures to protect those resources from malicious software infections including but not limited to virus and spyware.

This policy outlines how malicious software might infect University resources, how the IT department tries to prevent and/or minimize infections, and how University users should respond to viruses or spyware if they suspect infection of the network or University equipment.

BACKGROUND

There are various types of computer viruses: true viruses, Trojan horses, and worms. True viruses actually hide themselves, often as macros, within other files, such as spreadsheets or Word documents. [Note: Viruses can actually hide themselves in a variety of mediums: applications, boot sectors, partition sectors, etc.] When an infected file is opened from a computer connected to the University network, the virus can spread other resources and may do damage.

There are several types of spyware including, Adware, Browser Hijackers, and Keyboard Loggers. The purpose of Adware and Browser Hijackers is to track your browsing habits and sell that information to marketing companies. The user receives unsolicited popup ads while connected to the internet and may experience a change in default home page and search engine. Keyboard loggers are designed for one thing – theft of sensitive information. A Key Logger logs anything you type from your keyboard including passwords, and reports that activity back to the infiltrator.

Viruses and spyware pose SIGNIFICANT security threats and could enter the University network in a variety of ways:

- **E-mail**—By far, most viruses are sent as e-mail attachments or links. Attachments can be working documents or spreadsheets, or they might be viruses disguised as pictures, jokes, etc. Links may take you to a sight that will download a virus or spyware to your computer.
- **Disk, CD, Zip disk, or other media**—Viruses can also spread via various types of storage media. As with e-mail attachments, the virus could hide within a legitimate document or spreadsheet or simply be disguised as another type of file.
- **Software downloaded from the Internet**—Downloading software via the Internet can also be a source of infection. As with other types of transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file. Media or links shared via social media applications like FaceBook may also propagate infections.
- **Instant messaging attachments**—Although less common than viruses in e-mail attachments, more viruses are taking advantage of instant messaging software. These attachments work the same as e-mail viruses, but they are transmitted via instant messaging software. See "Instant Messaging."

POLICY

It is the responsibility of all users to take reasonable steps to prevent virus outbreaks. Use the guidelines below to do your part:

* Do not open suspicious or unexpected e-mail attachments, even from coworkers. It is possible to "spoof" legitimate email addresses.
* Never open an e-mail or instant messaging attachment from an unknown or suspicious source.
* Never download freeware, shareware, or other software from the Internet without express permission of the IT department.
* If a file you receive contains macros that you are unsure about, disable the macros.
* If you suspect a virus or spyware and are unsure as to how to proceed, contact the IT department.

MINIMIZING THREATS

Scanning Internet traffic—All Internet traffic on our network must pass through Hodges servers and other network devices. Only specific types of network traffic are allowed through the University's firewalls.

Running server and workstation antivirus and antispyware software—All servers run antivirus and antispyware scanning software. This software scans our systems, looking for suspicious code. Antivirus and antispyware protection software is also installed on all University workstations. This software scans all data written to or read from a workstation's hard drive. If it finds something suspicious, it isolates the dubious file on the computer, alerts the user and IT.

Routinely updating virus and spyware definitions—University virus and spyware scanning programs check the program's control center for updated definitions on a regular schedule. These definition files allow the software to detect new viruses. If a new virus definition file is available, the virus scanning software is automatically updated.

Regularly scheduled full system scans—In addition to on-access and other scans that are run regularly during daily computing tasks, computers are scheduled to run full nightly scans for viruses and spyware.

REPORTING A VIRUS

Although the University takes appropriate precautions to protect our servers and workstations, the possibility still exists that a virus could find its way to an employee's workstation and if not properly handled, could infect and potentially expose University resources.

The IT staff will attempt to notify all users of credible virus threats via established communication methods. On occasion, well-meaning people will distribute virus warnings that are actually virus hoaxes. These warnings are typically harmless; however, check with IT as to the validity of these warnings.

Notify the IT Department of Suspicious Files or Infections If you receive a suspicious file or e-mail attachment, do not open it. Submit a help desk ticket indicating that you have received a suspicious file. IT will contact you to explain how to handle the file. If University anti-virus software alerts you that you have a virus, contact IT immediately.

If the potentially infected file is on removable media that you have inserted or connected to your computer, the antivirus software on your machine may ask you if you wish to scan the media, format the media, eject the media, or delete the file. Safely remove or eject the media and submit a help desk ticket. IT will contact you to instruct you as to how to handle the removable media.

After IT has neutralized the file, send a note to the person who sent/gave you the file notifying them that a virus was detected. (If the file was sent via e-mail, the antivirus software running on our e-mail system will automatically send an e-mail message informing the sender that a virus has been detected.) If the file is an infected spreadsheet or document that is of critical importance to the University, the IT department will attempt to scan and clean the file. The IT department, however, makes no guarantees as to whether an infected file can be totally cleaned and will not allow the infected file to be accessed on University resources.
Passwords

PURPOSE

Passwords are the entry point to University resources. Protecting access to resources is critical in ensuring that our systems and our constituent’s sensitive information remain secure. The University must be diligent in guarding access to resources and protecting them from both internal and external threats.

POLICY

This policy outlines the handling, responsibilities, and scope of passwords for the Information Technology (IT) resources of Hodges University. The policy objective is to enable University employees to perform their tasks while appropriately addressing business needs and keeping information secure. This policy addresses passwords for all IT managed systems.

PASSWORD HANDLING

Passwords for all systems are subject to the following rules:

- Passwords are not to be displayed or concealed on your workspace.
- IT may on occasion ask you for your password while troubleshooting issues based on a request initiated by the user. Other than this instance, no passwords are to be spoken, written, e-mailed, hinted at, shared, or in any way known to anyone other than the user involved. This includes supervisors and personal assistants.
- Users may receive phishing emails from outside sources with the intent of gaining access to University systems to be used in a malicious or unapproved manner. NEVER respond to any generic email requesting username or password. IT will never send unsolicited bulk or individual emails of this kind!
- No passwords are to be shared in order to "cover" for someone out of the office or for any other reason.
- Passwords are not to be shared with work studies for any reason.
- Local, administrative, and/or BIOS passwords set by IT are not to be in any way modified.

PASSWORD COMPOSITION

The University Information Technology department uses various methods of password enforcement. All windows/network password creation is restricted by the following rules (last updated 5/09):

**Staff Password Policy:**
- Password must be changed every 60 days
- 8 Character Minimum
- 2 Character Set Minimum
- Cannot contain username
- Cannot contain parts of full name
- Cannot contain words in our custom dictionary
- Must not use any one of the 5 last passwords

**Student Password Policy:**
- Password must be changed every 120 days
- 8 Character Minimum
- 2 Character Set Minimum
- Cannot contain username
- Cannot contain parts of full name
- Cannot contain words in our custom dictionary
- Must not use any one of the 5 last passwords
Users with access to sensitive or confidential information are subjected to a more stringent password standard.

**Power Users, IT and Administrative Policy:**
Password must be changed every 30 days
8 Character Minimum
3 Character Set Minimum
Cannot contain username
Cannot contain parts of full name
Cannot contain custom dictionary words
Special characters restricted to !@#$%^&*()-_
Must not use any one of the 5 last passwords

**RESPONSIBILITIES**

All Hodges University users are responsible for complying and implementing this policy. IT has the responsibility to enforce this policy. This will be done through systematic means and interaction with users.
Data Backup and Restoration

PURPOSE

The Hodges University backup policies are intended to protect data on IT managed systems and ensure timely, accurate recovery of data from network resources in the event of a hardware failure, software failure, data corruption, natural disaster or user error.

The IT department recommends that all users store important University information on their assigned network share – traditionally the I:\ drive. Each full time Hodges employee is assigned a network share upon commencement of their employment. These shares may be accessed remotely using University provided VPN client software or more commonly through the I:\ drive web part accessed through the MyHUgo portal. These network shares are backed up as part of the regular backup schedule ensuring data continuity and availability in the event of a local failure.

BACKUP SCHEDULE

Full backups of network resources are run based on the following schedule:

1) Incremental backups to disk are performed Sunday through Thursday. These backups are on a 30 day with 3 cycle rotation (90 days split among 3 sets) after which, the oldest will be overwritten.

2) A full weekly backup to disk is performed on Fridays. On Sundays the latest full backup to disk will be copied to tape. These weekly full backups are on a 4 week 3 cycle retention (12 weeks total split among 3 sets) after which, the oldest will be overwritten. These tapes are stored offsite.

3) A full end of the month backup is performed strictly to tape each month. These tapes are on a one year retention and are kept offsite.

Backups are monitored daily. Backup log files are reviewed each morning for errors. In the event of an error, corrections are made.

DATA RESTORATION POLICY

In the event that data restoration is required, a user must submit a helpdesk ticket including the date, path, filename, reason and place for restoration. Data should not be restored to original location – to prevent overwriting of existing data. Typically, restores are done to the user’s network share.
Universal and eWaste Disposal

BACKGROUND AND DEFINITIONS

Universal Waste: Hodges University manages the four (4) post-consumer used wastes (i.e. universal wastes), listed below, under either the less stringent Universal Waste Management Standard. The four (4) universal wastes include:

- Used batteries that exhibit one or more of the hazardous waste characteristics listed in 40 CFR Part 261, Subpart C, including spent lead-acid batteries;
- Pesticides that are stocks of suspended or cancelled pesticides or unused pesticides;
- Used mercury-containing equipment that exhibits one or more of the hazardous waste characteristics listed in 40 CFR Part 161, Subpart C, including mercury thermostats; and
- Used mercury-containing lamps that exhibit one or more of the hazardous waste characteristics listed in 40 CFR Part 261, Subpart C.

Under the Universal Waste Management Standards, a generator of universal wastes at a minimum must:

- Manage universal waste in a way that prevents release of any universal waste or component of a universal waste into the environment;
- Label or mark each universal waste or each container of universal waste with one of the phrases listed in 40 CFR 273.14;
- Demonstrate the length of time that the universal waste has been accumulated on-site; and
- Accumulate universal waste on-site for no longer than one (1) year.

The Code of Federal Regulations [40 CFR 273.14] states that a small quantity handler must of universal waste must label or mark the universal waste to identify the type of universal waste as specified below (only relevant waste statements excerpted from [40CFR 273.14]):

(a) Universal waste batteries (i.e., each battery), or a container in which the batteries are contained, must be labeled or marked clearly with any one of the following phrases:
   a. “Universal Waste—Battery(ies)"
   b. “Waste Battery(ies)"
   c. “Used Battery(ies)"

(e) Each lamp or a container or package in which such lamps are contained must be labeled or marked clearly with one of the following phrases:
   a. “Universal Waste—Lamp(s)"
   b. “Waste Lamp(s)"
   c. “Used Lamps"

E-waste: E-waste is a general category for electronic products facing displacement or replacement that are hazardous due to the toxic metals present within their internal materials, coatings and glass. E-waste may include personal computers, monitors, televisions, keyboards printers, telephones, typewriters, calculators, copiers, fax machines and audio equipment. There are commodities worth capturing in E-waste; plus, there are traditionally toxic materials in electronics that should be kept out of the environment and properly managed.

The State of Florida does not have a separate E-Waste Regulation and thus, it must either be recycled or disposed as hazardous waste after proper hazardous waste determinations have been made.
DISPOSAL PROGRAM OVERVIEW

Hodges has a recycling program for E-Waste (computer equipment) and IT Universal Waste (certain batteries and lamps) operated through the IT Department for both campuses. Hodges maintains their E-waste and IT Universal waste in secure storage rooms - AV Rooms located at both the Fort Myers and Naples campuses. The storage rooms are the campus centralized area for the collection, storage, and packaging for off-site recycling of E-waste and IT Universal Waste. Hodges recycles their E-Waste and Universal Waste through Waste Paper Technologies, and maintains all certificates of recycling in on-site files.
IT Access to Offices

PURPOSE

The IT department is trusted with the ability to access most areas due to the nature of their responsibilities. Although IT staff is trained to understand information privacy, confidentiality and respect for personal space, it is understood that certain areas or workspaces may contain confidential or personal information and that employees may wish to prepare their area if an IT visit has been requested in their absence.

POLICY

When a staff member requests IT support, the user must specifically permit the IT department access to their office if the work is to be performed in their absence. In the event of an emergency, IT is empowered to enter offices and do what is necessary to protect University resources.

PROCEDURE

In the event that work is requested to be performed in an employee’s absence the following procedure applies:

1. A helpdesk ticket must be submitted indicating permission for IT to enter the office while the employee is not present.

2. If IT was not given permission to enter the office via a helpdesk ticket, IT will try to setup an appointment to complete the requested work at the user’s convenience.
   
   Note: If IT is having trouble finding a convenient time for the employee, IT will ask for verbal permission to enter the office in the user’s absence and will record this in the helpdesk ticket.

3. IT will not touch any materials in the office other than the computer, and will consider anything in plain view to be private and confidential.

4. IT Staff will leave a note indicating they have performed the requested work.

5. When the requested work is complete, the office will be left as it was and the office door will be locked.
Access to Network Rooms and IT Storage Areas

PURPOSE

Although the University enforces strict access controls to information and systems, physical security is the basis of all security. Many users require master keys for the performance of job duties, having access does not necessarily constitute privilege to access. This policy has been developed to restrict access to:

1. Secure areas and therefore limit possible information leaks, accidents, negligence, or malicious attacks.

2. IT Storage areas to ensure accurate accounting and control of assets based on established procedure.

POLICY

It is strictly forbidden for any non-IT personnel to access secure areas such as the Network rooms on each campus or IT storage areas without express permission from the Director of IT. Exceptions include:

1. Certain Facilities Management staff may have access to these areas for the express purpose of maintaining facilities infrastructure such as air conditioning.

2. University Administration.

Other activities or access other than noted above are prohibited.
Requesting IT Assistance

POLICY

In order to assure prompt and efficient resolution of user requests and ensure IT staff and their classmates are not disturbed while in class, the following procedures must be followed when requesting IT assistance. These policies are in place to ensure a consistent level of support.

EMPLOYEES

Classroom Technical Assistance: Should a user require immediate technical assistance during class hours, use a hall phone to contact the reception desk. IT provides reception desks at both campuses a schedule of IT staff hours. If the need is not immediate and can wait approximately 24 hours, submit a helpdesk ticket.

Event Technical Assistance: Should IT assistance be required for an upcoming event, submit a helpdesk ticket 2 weeks prior to the event, if possible. This allows staff time to plan for off hours events and collect necessary resources.

Other Technical Assistance: It is IT policy that all IT related requests/issues be communicated through a helpdesk ticket. This allows any staff member to handle the request regardless of who may or may not be available at that time.

Please Note: A technical emergency of any kind does not constitute the right to pull any IT staff member from his or her classes. *When a staff member is in class he/she is to be treated as a student!*

STUDENTS

Students requesting technical assistance will be required to identify themselves based on the currently adopted [Student Identification Procedure](#). Several methods are available for students to contact the IT department. The IT department posts this information in the Portal, on the website and informs students during orientation.

Student requests/issues that are escalated from our 24x7 helpdesk or are handled by on-site IT staff will be responded to within 24 hours on weekdays and within 48 hours on the weekends.

OTHERS

IT may help outside constituents using our facilities gain access to our wireless network or connect to our AV equipment.

In order to protect IT staff and the University, it is the policy of the IT department NOT to provide technical assistance beyond situations noted in these policies, unless a special provision has been made by administration.
Remote Access

PURPOSE

Hodges University provides remote access to certain network resources through the use of a secure Virtual Private Network (VPN). This places the user’s computer on the University network from an internet connection which introduces certain security risks to the Hodges network.

Remote users such as home users and off-site users must use the VPN when connecting to certain client/server applications. Although most applications are available through a web interface, many users prefer using the client.

This policy is meant to protect University data and resources.

POLICY

1. The VPN client may be installed upon Supervisor request for any employee.

2. For security reasons the VPN software MUST be used by Learning Site employees that operate on an outside network.

3. VPN software cannot be installed on non-IT managed (i.e. personal) equipment. Doing this could introduce viruses and other unknown complications to University resources.

4. The University may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.
Equipment Usage

PURPOSE

The Information Technology department is charged with procurement, maintenance, and tracking of University technology assets. IT has established vendor relationships to the benefit of Hodges University as well as tracking procedures and maintenance schedules to protect University assets. In order to ensure appropriate supervisory control and accurate inventory, the following policies have been established.

POLICIES:

EQUIPMENT LENDING AND NEW EQUIPMENT REQUESTS

Supervisors must request new equipment using the ticketing system or a Capital Budget Request form (during the budget planning cycle) for equipment valued over $500. Purchases will not be made without the completed form.

All IT equipment of a significant value (over $199) is to be recorded in the IT asset tracking system.

IT EQUIPMENT PURCHASES

To ensure that all equipment conforms to current University standards, is purchased at the best possible price, and is supportable, all technology purchases should be made through the IT Department. IT may recommend that purchases of a nominal amount (to be determined by IT) be made by the requesting department. Equipment requests will be handled on a case by case basis and must be approved by the IT Department. No purchases can be made by IT without the approval of the Director of IT.

PERSONAL HARDWARE

Although the IT department will make recommendations as a professional courtesy with no implied warranty or liability, personal hardware will not be maintained, worked on, or upgraded by the IT department.

Hodges University provides assigned or accessible equipment and software to its employees. Employees are NOT encouraged to use personal software or equipment on campus. Misuse or damages to personal equipment connected to Hodges University resources are the sole responsibility of the employee.

SOFTWARE INSTALLATION

This policy is designed to allow University employees to achieve their business objectives while minimizing system downtime and the need for IT support. Full cooperation with this policy is appreciated in order to maintain and acceptable level of service and support and to ensure goals can be met in accordance with the University mission.

The IT Department prohibits the installation of non-University licensed software on University laptops. The introduction of untested software can result in poor performance and a variety of issues including compatibility with University licensed software. Should a situation arise requiring the installation of personally owned software on a University computer, the request must be approved by the supervisor and the Director of IT. In addition, the software owner must sign a waiver verifying licensing.
Software requests: If a user is to request software for his/her University assigned computer, the proper procedure is to complete a helpdesk ticket. Requests for classroom software should be completed using the Software for Semester Form and will be requested each semester by the IT staff with a deadline to ensure timely installation of classroom computers for the upcoming term.

Note: Requests submitted after the stated deadline may delay installation and availability of the software.

MAINTENANCE

Maintenance or troubleshooting of Hodges provided equipment by any party other than the IT Department staff or approved contracted vendors is strictly prohibited. Maintenance by other parties may negate warranties, violate leasing agreements, and/or introduce threats to the University network.

In an effort to ensure operability, efficiency, and security of University resources all laptops will be surrendered to the IT department twice yearly to undergo routine maintenance. An ongoing schedule has been established. Users will be notified when their laptop is due for regular maintenance.

EQUIPMENT RELOCATION

The known location of computing equipment is important in troubleshooting and in the inventory and reporting of University assets. Therefore, all relocation of technology equipment must be executed or coordinated by the IT Department.

No assigned equipment can be lent or transferred to another party without knowledge and prior approval of the IT Department.

EMPLOYEE EQUIPMENT RESPONSIBILITIES

All hardware acquired on behalf of the University including University assigned equipment remains the property of the University. Employees borrowing a University laptop or other IT equipment are solely responsible for its condition. All laptops may be taken off the University premises unless specifically stated otherwise. Abuse of equipment may result in financial liability and prohibition from further use of resources.

Desktop PC’s may not be taken off University premises.

Users leaving employment with the University must return all equipment to the IT Department and are responsible for ensuring that it has been marked as received on the Employee Exit Form. Equipment that has not been returned upon termination of employment may be remotely wiped and reported as stolen.

Adjunct Faculty on hiatus and staff on leave must relinquish ALL IT equipment.

BLACKBERRY AND CELL PHONE USAGE

In an effort to ensure efficient customer services and timely communication amongst its employees, Hodges University provides Blackberry devices or other cell phones to authorized employees. Although it is understood that some personal use may take place, it should be done in a reasonable and judicious manner.

Authorized Employees

Cell phones will be distributed to staff and faculty that meet at least one of the following requirements:

1) Hold a title of Director or Program Chair or above and supervise 2 or more employees.
2) Hold a position that requires them to be “on-call” (e.g. Facilities, Internship Coordinators, and Distance Education Admissions Representatives).

To ensure privacy of organizational data and communications, smart devices are set by IT to be password protected and should not be altered to nullify this setting.

Users should not elect additional paid services or download additional software to their assigned cell phone or Blackberry. Users who do may be subject to charge backs.

IT will provide one charger that ships with the phone for each cell phone issued. Additional chargers must be purchased by the user.

In the event that a Blackberry is lost or stolen, notify IT immediately and the device will be remotely wiped.
Staff Equipment Distribution

PURPOSE

Staff members (below VP level) who have an assigned office at a campus are currently provided with a Hodges' assigned desktop pc configuration. Some who travel regularly between campuses have a pc at both campuses. Many staff travel regularly between campuses and have opted to trade in their desktops for a laptop to better accommodate their mobility and pc needs. In the past some staff members were in possession of more than one desktop as well as a laptop and some who do not travel regularly were also in possession of a desktop and a laptop.

POLICY

It is the position of the IT department and University Administration that if a staff member travels regularly between campuses/learning sites or works frequently from home or requires a VPN connection in order to complete their work, they may request a laptop. We do not install VPN software on home PCs, as it places that pc on our network and we have no way of ensuring up-to-date antivirus, etc. on personal PCs. A University issued laptop is the only alternative. If staff members travel regularly between campuses/learning sites, they should request a laptop in lieu of a desktop at each location. The following configurations are offered for these scenarios:

1) Multiple campuses and/or authorized home use: docking station at both campuses with laptop.
2) Single campus and occasional home use: desktop on campus and request a loaner laptop as needed.

This policy has been adopted to control Hodges University IT expenditures and hardware sprawl, as well as software and hardware maintenance costs.

A change of employment status, position or leave may result in a re-evaluation of equipment needs.

*This policy was approved by Hodges University Administrative Council on September 23, 2008.

EXCLUSIONS

This policy does not apply to individuals with shared desktops/laptops. In addition, this policy does not apply to IT staff that have additional responsibilities necessitating secure (VPN) access to the network on a continuous basis to perform their assigned duties.

DESKTOPS

Each full time staff member who is currently assigned a laptop as well as a desktop pc, will have the choice between a single desktop pc or a laptop only configuration.

LAPTOPS

Laptops will be distributed to staff based on the above configuration options. To facilitate productivity with laptop only configurations, staff will be given the option of using a docking station with a mouse, keyboard, and monitor. In the event that a staff member falls under scenario number 2 above or is required to travel on University business, a loaner laptop is available for temporary use from IT. Staff members on leave must return all IT equipment that has been allocated to them.
MIFI DEVICES

Although most hotels now provide internet access, MiFi devices are provided for temporary use during travel only. They are not intended to replace a personal internet connection.

IT will not troubleshoot personal internet connections or “home use” networks or equipment.

PRINTERS

Printers will be assigned to those employees that are not within comfortable walking distance of a copy machine or shared printer and can demonstrate appropriate need. Secure printing and scanning are available on every copy machines and are not justification for a personal printer.
Faculty Equipment Distribution

PURPOSE

Faculty members (Program Chairs, Directors, Faculty) who have an assigned office at a campus are currently provided with a Hodge’s assigned desktop pc configuration. In the past, some faculty members have opted to trade in their desktops for a laptop to better accommodate their mobility and pc needs. Other faculty members were in possession of both a desktop and a laptop.

POLICY

It is the position of IT that being a campus connected faculty member who also happens to teach online is not in and of itself sufficient justification for the allocation of a separate and permanent laptop to that faculty member. It is that faculty member’s responsibility to either use his assigned office pc or his personal home pc to accomplish his teaching duties. All Hodges services are available online through a standard web browser. Microsoft Office home use media can be licensed by current staff and faculty. The suite may be purchased online through the HU Central team site.

If a full time faculty member teaches exclusively at a distance and is not allocated a campus office then a Hodge’s laptop may be provided to that faculty member.

This policy has been adopted to control Hodges University IT expenditures and hardware sprawl, as well as software and hardware maintenance costs.

A change of employment status, position or leave may result in a re-evaluation of equipment needs.

*This policy was approved by Hodges University Administrative Council on August 12, 2008.

DESKTOPS

Each full time faculty member who is assigned a campus office will have the choice between a single desktop pc or a laptop only configuration.

LAPTOPS

Laptops will be distributed to campus connected faculty only in lieu of using a desktop pc. To facilitate productivity with this laptop only configuration, faculty will be given the option of using a docking station with a mouse, keyboard, and monitor at their primary office location. In the event that a faculty member who is using a desktop pc is required to travel on University business a loaner laptop is available for temporary use from IT. Laptops will not be distributed to adjunct faculty except on a temporary loaner basis.

A change of employment status, position or leave may result in a re-evaluation of equipment needs.

Adjunct faculty who are on semester hiatus must return all IT equipment that has been allocated to them.

MIFI DEVICES

Although most hotels now provide internet access, MiFi devices are provided for temporary use during travel only. Because a faculty member teaches online is not justification for allocation of a MiFi device. Faculty members who teach online should have an appropriate internet connection at home.
IT will not troubleshoot personal internet connections or “home use” networks or equipment.

PRINTERS

Printers will be assigned to those employees that are not within walking distance (on the same floor) of a copy machine or shared printer and can demonstrate appropriate need. Secure printing and scanning are available on every copy machines and are not justification for a personal printer.
Computer Lab Usage

PURPOSE

The policies below are meant to ensure equitable use of available resources to all students as well as an environment conducive to academic achievement.

POLICY

1. Always sign into the lab.
2. Computers may be used on a first come, first served basis.
3. One person per computer.
4. One hour maximum when others are waiting.
5. Please work quietly.
6. No eating or drinking in the lab.
7. Please clean up your workspace when you leave.
8. Children are not permitted in the lab.
9. Please do not download anything from the Internet to the lab computers.
10. Do not load software of any kind on computers.
11. Please do not move computer equipment for any reason.
12. Please do not add, delete or move any icons on the desktop.
13. All removable media will be automatically scanned on use.
14. Put cell phones on vibrate and leave the lab to talk should you need to take a call.
15. Tutoring sessions or Group Study sessions are to be held in the Library Study Rooms or AAS Tutor rooms, not in the Computer Lab.
16. Print jobs over 20 pages long should be printed to the library copy machine.
17. Use of Instant Messaging Software, (AIM, Yahoo, MSN, etc.) gaming and downloading of personal media of any kind is strictly prohibited.

ENFORCEMENT

Because the above policies are critical to the success of students using the computer lab for academic pursuits, IT staff is empowered to enforce the above rules as follows:

First Infraction: a polite friendly warning will be issued by the IT staff member present. User will be directed to Computer Lab Policies for review.

Second & Third Infraction: an additional polite, friendly warning will be issued by the IT staff member present and the user will be informed that this is his or her second/third infraction. User will once again be directed to Computer Lab Policies for review. Student name and id number will be recorded in lab infraction log for purposes of documentation.

Fourth Infraction: the student will be asked to leave the computer lab and will be directed to Executive VP of Academic Affairs to have lab privileges reinstated. The IT Department will be informed that this student’s lab privileges have been revoked until IT is notified otherwise by the Executive VP of Academic Affairs. The infraction log will be updated with the fourth infraction.

Reinstatement: once notified by the Executive VP of Academic Affairs that the student)’s lab privileges are to be reinstated, this will be recorded in the infraction log, and the IT Department will be notified of reinstatement. Should the student request lab privileges before IT has been notified of reinstatement, the student will be directed to the Executive VP of Academic Affairs.

Hodges University reserves the right to revoke computer lab privileges in the interest of minimizing distractions for all students and enforcing an environment conducive to academic achievement.
Computer Classroom Usage

PURPOSE

The policies below are meant to ensure security and equitable use of available resources for all students and faculty as well as an environment conducive to academic achievement.

POLICY

1. Students are not to be in computer classrooms unattended.

2. Computer classrooms are to be locked when not in use. Classrooms will be unlocked 10 minutes prior to class start.

3. No food or drinks are allowed.

4. While in the computer classroom, instructors should make students aware that they should be using the technology in the classroom only as it directly relates to the material being discussed.

5. Use of Instant Messaging Software (AIM, Yahoo, MSN, etc.), gaming and downloading of personal media of any kind is strictly prohibited.

6. IT staff are available on site until 7:30 p.m. Monday through Friday – on the campuses that offer Friday courses.

7. If you have a computer emergency during class call the reception desk for your campus via a hall phone. Reception has an updated IT staff schedule and will contact an IT staff member for you. All IT staff contact information is available at the reception desks on both campuses.

8. If you require service (non-emergency) on any classroom equipment, submit a helpdesk ticket at your convenience.
### Student Laptop Usage

#### PURPOSE

This policy is intended to protect the University and to ensure that students receive adequate access to the University wireless network using their personal laptops. All policies listed apply both to the use of resources on or off campus.

#### POLICY

1. Hodges University is not responsible for damage to student equipment when used in conjunction with the University network or other technology resources.

2. It is the responsibility of the IT department to provide students with basic information required to log on to the University student wireless network. **No other assistance with student's personal equipment is permitted.**

3. Students who use the network should have some form of up-to-date anti-virus and anti-spyware software on their laptop – for their own protection.

4. Although using their own equipment, students, while on campus, must adhere to University **Acceptable Use of Technology Resources** policy.

5. Determination of what the student will have access to and where is determined by the Information Technology Department in conjunction with University administration. Whether connecting to the network or for general use, student laptop usage may be confined to certain locations.

6. All registered students will be provided a Hodges University email account (see [Email Usage](#) policies for details). It is the responsibility of the student to check this assigned email account for notifications and information concerning changes to or availability of University technological resources.

7. The University regularly conducts maintenance of its resources which may require service interruptions. The University makes no guarantee of service availability.

8. Some lab study aids, and classroom software must be accessed on-site through a University computer.

9. The University regularly monitors network traffic for unauthorized or unacceptable use and reserves the right to terminate or restrict access to the network or other resources at any time for maintenance or if there is a danger to the integrity of the network.

#### MONITORING AND ENFORCEMENT

**Monitoring:** The Information Technology Department of Hodges University, while managing the operation of computers and networks, may routinely monitor and log usage data. These persons may review this data for evidence of violation of law or policy, and other purposes. The use of the University student wireless network implies agreement with University monitoring policies.

With authorization, the Director of IT may monitor the activities of and inspect the files of users. University officials reserve the right to access and examine the files and/or actual network activity of any user to investigate violations or suspected violations of security and/or policies. For this reason, users...
must regard themselves as having no expectation of privacy with regard to their file, electronic activities, data or communications.

**Enforcement:** Students must adhere to all applicable acceptable use policies. In the event that a violation is suspected or has been reported, penalties may range from termination of access up to and including dismissal and legal action.
Work Studies, Volunteers, and Interns

PURPOSE

The Hodges University IT Department welcomes the use of Hodges University work-study students and interested volunteers. This can be a beneficial professional relationship in which the volunteer receives valuable training and experience in exchange for assisting with the IT Department workload.

POLICY

Since volunteers are applying from outside the University, the student’s instructor in his/her respective school or training program will be called for a reference.

Work-study students and volunteers will be identified to school staff and faculty via e-mail at the beginning of the semester that they are working, including name, contact information and work hours.

IT work-study students and volunteers are required to wear a name badge identifying them as such at all times while on duty.

Work-study students and volunteers are bound by all Hodges University IT department policies and procedures and sign the standard confidentiality agreement as well as the form at the end of this document and are forbidden access to University systems without prior approval.

Hodges University employees are not to share any personal access information with work studies, volunteers or interns for any reason whatsoever.

See University Work-study, Tutor and Teaching Assistant Policies
Student Laptop Lending Program

PURPOSE

Hodges University makes non-classroom computer resources available to its onsite students via our computer labs and libraries. The University requires that students who take online courses or that are enrolled in an online program own a computer. While these practices cover most student needs, it is understood that on occasion a student may lose access to their home computers because of unanticipated repairs, upgrades, etc. In order to assist students during the temporary loss of their PCs the University makes a limited number of laptops available to on campus students through a laptop lending program administered by the IT Department in its computer labs.

The purpose of this policy is to establish guidelines for the lending program.

POLICY

The number of laptops available for lending may change without notice. Laptops will be lent to students that have a signed Student Laptop Lending Request Form from their instructor. Instructors will not approve these requests as a permanent replacement for a student’s personal PC access. Laptops will be checked out for a two week period and will be distributed to the next student on the waiting list upon return. To ensure equitable distribution of limited resources, no exceptions will be made to this policy.

Hodges University will not be held responsible for:

- Unrecoverable information or documents left on the laptops
- Viruses, spyware, and associated repairs transferred between loaner laptops and other PCs
- Absences or missing classwork related to unavailability of loaner laptops
- Lost classwork or other information rendered unavailable due to the locking of the laptops when not returned at the end of the checkout period

Hodges University will not ship or deliver laptops and reserves the right to end this program at its discretion.

PROCEDURE

The IT Department will track laptop distribution on its team site. Students that have not returned the laptops by the conclusion of the two week check-out period will be contacted via email that the laptop will be locked if not returned within five days and reported stolen if not returned within seven days. Tracking software is installed on all loaner laptops.

Laptop Setup

All software will adhere to the current versions in use by Hodges. The laptops will be equipped with minimal software as follows:

- Microsoft Office
- Internet Explorer
- Deep Freeze
- McAfee Anti-Virus
- Spybot Anti-Spyware
- Computrace
In addition the laptops will be outfitted with the following:

- Wireless Access
- External Mouse
- ‘Unfrozen’ Document Directory

**Laptop Maintenance**

Returned laptops will undergo the following maintenance before being checked out again:

- Deletion of files in 'unfrozen' directory
- Full virus scan
- Full spyware scan
- General cleaning
Violations

REPORTING VIOLATIONS

Any violation of these policies poses an unacceptable risk to the University, its reputation and its constituents. Violations must be reported immediately to an immediate supervisor, the Director of IT, or a member of University Administration.

INVESTIGATION

If a supervisor has reasonable cause to believe or has received a report that an activity prohibited by IT policy is being engaged in by an employee, the supervisor should notify the Director of IT or a member of University Administration.

The Director of IT will obtain authorization from University Administration to monitor the employee's activity. The Director will then use any and all tools at their disposal to implement monitoring. Should this require involvement of other IT staff, confidentiality will be strictly maintained by those involved.

Monitoring will take place long enough to prove or disprove alleged infraction to the satisfaction of IT, the Supervisor and University Administration. Data gathered through monitoring will be kept confidential but will be made available to the Supervisor and/or University Administration as required.

University Administration may inform the employee whose network activity is being examined of the reason for the investigation as soon as is practical.

The Director of IT in conjunction with University Administration reserves the right to enforce IT policies according to all applicable Violation, Enforcement, and Monitoring sections of this document, the Acceptable Use of Technology Resources Policy.

PENALTIES

Violations will be reviewed on a case-by-case basis. If it is determined that a user has violated one or more of these acceptable use policies, that user will receive a reprimand from his or her supervisor and his or her future use may be closely monitored. If a gross violation has occurred, University Administration will take appropriate action. Such action may result in losing access privileges, severe reprimand, terminating employment, and legal action which may include restitution for damages.
*Acceptance

Your signature indicates that you have read and understood Hodges University’s Acceptable Use of Technology Resources policy. Your signature does not mean that you agree with each and every provision of the policy. However, it does indicate that you will abide by the regulations set forth in the above policy as well as future revisions of the policy.

Printed Name: ______________________________________________________________

Employee ID: ____________________ Date: _________________________________

Signature: __________________________________________________________________

*This signature page is to be filed in the employee’s HR file.
RELATED DOCUMENTS
Academic Honesty Policy
Email Best Practices
Information Assurance Policy
Student Laptop Lending Request Form
Web Editorial Policy
Student Identification Procedure
Media Duplication/Home Personal Use Software Installation Request Form
Media Duplication and Home/Personal Use Software Installation Request Form

This policy is intended to protect Hodges University from negative repercussions resulting from the duplication of copyrighted electronic media, such as movies or software in DVD/CD format. Before the IT Department can handle your duplication request, certain requirements must be met, depending on the type of media being duplicated.

Media Duplication
For copyrighted works such as VHS or DVD videos, documentation stating that the owner has permission to duplicate the work must be attached to a signed copy of this form. This documentation should be submitted to the Multimedia Technologist for approval prior to the work being done.

By signing below, you acknowledge that:

You received permission to copy the media from either the originating copyrighter, or from an authorized “Copyright Clearance Center.”

You agree to use the duplicated material(s) in a strictly educational environment.

Home/Personal Use Software Installation
For University software that has a license permitting installation on home computers, this form must be signed. Please note that the IT Department cannot provide technical support on home computers and cannot be held responsible for University provided software damaging your computer or conflicting with other software.

By signing below, you acknowledge that:

The software will only be installed on one personal computer.

You agree to use the duplicated material(s) strictly for educational purposes.

By neglecting to abide by the above policies, the user holds him/herself legally responsible for any negative repercussions that may result from abusing copyrighted materials.

Title of work ______________________________________________
Format of original ______________________________________________
Format being copied to ______________________________________________
Copyrighted by / Year ______________________________________________
Purpose for duplication ______________________________________________

Signature ______________________________________________
Date _____________