Student Acceptable Use of Technology Resources
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Department Vision, Mission, and Principles</td>
<td>5</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>Purpose</td>
<td>6</td>
</tr>
<tr>
<td>Authority</td>
<td>6</td>
</tr>
<tr>
<td>Continuance</td>
<td>6</td>
</tr>
<tr>
<td>Scope</td>
<td>7</td>
</tr>
<tr>
<td>Definitions</td>
<td>7</td>
</tr>
<tr>
<td>Administrative Rights and Privileges</td>
<td>8</td>
</tr>
<tr>
<td>Permitted Use of Resources</td>
<td>9</td>
</tr>
<tr>
<td>Prohibited Use</td>
<td>9</td>
</tr>
<tr>
<td>Student Identification Policy</td>
<td>11</td>
</tr>
<tr>
<td>Responsibilities</td>
<td>11</td>
</tr>
<tr>
<td>Unauthorized Access</td>
<td>11</td>
</tr>
<tr>
<td>Termination and Review of Individual Access</td>
<td>12</td>
</tr>
<tr>
<td>Account Audits</td>
<td>12</td>
</tr>
<tr>
<td>User Privacy</td>
<td>12</td>
</tr>
<tr>
<td>Copyright, Intellectual Property, and Software Use</td>
<td>13</td>
</tr>
<tr>
<td>USE OF LICENSED SOFTWARE</td>
<td>14</td>
</tr>
<tr>
<td>Peer-to-Peer and File Sharing</td>
<td>15</td>
</tr>
<tr>
<td>PURPOSE</td>
<td>15</td>
</tr>
<tr>
<td>POLICY</td>
<td>15</td>
</tr>
<tr>
<td>LIABILITY</td>
<td>15</td>
</tr>
<tr>
<td>DISRUPTION OF SERVICES</td>
<td>15</td>
</tr>
<tr>
<td>SECURITY</td>
<td>16</td>
</tr>
<tr>
<td>PRIVACY</td>
<td>16</td>
</tr>
<tr>
<td>Streaming Media</td>
<td>17</td>
</tr>
<tr>
<td>PURPOSE</td>
<td>17</td>
</tr>
<tr>
<td>POLICY</td>
<td>17</td>
</tr>
</tbody>
</table>
Student Laptop Usage ............................................................................................................. 27

PURPOSE .......................................................................................................................... 27

POLICY ............................................................................................................................... 27

MONITORING AND ENFORCEMENT .................................................................................. 27

Student Laptop Lending Program .......................................................................................... 29

PURPOSE .......................................................................................................................... 29

POLICY ............................................................................................................................... 29

PROCEDURE ....................................................................................................................... 29

Violations ............................................................................................................................. 31

REPORTING VIOLATIONS .................................................................................................. 31

INVESTIGATION ................................................................................................................ 31

PENALTIES ......................................................................................................................... 31

RELATED DOCUMENTS ...................................................................................................... 32

Academic Honesty Policy ................................................................................................... 33

Email Best Practices ........................................................................................................... 33

Student Laptop Lending Request Form ................................................................................ 33
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 constituents 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 students 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.

**Student**: Current or past student that uses any University electronic resources (e.g. email, library resources, etc.).
Administrative Rights and Privileges

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

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.

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

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.

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.

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.
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

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.
Student Identification Policy

It is the policy of Hodges University to protect its information assets in accordance with all applicable federal and state statutes and regulations, as well as with effective information assurance/security practices and principles generally accepted as ‘due diligence’ within the higher education community.

When requesting information in person Hodges University requires students to show a University Student Photo ID card before any information will be released. Requests made over the phone or via email require that students provide the last 4 digits of his or her Social Security number or Date of Birth as well as the Student ID number.

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.

**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.

**Account Audits**

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

**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
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.
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 student.
- Address any potential liability from instances when users 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 users 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 user’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 user’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 a user’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 a user’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 merit is prohibited.
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 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 user 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 cloud email 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
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 users of University resources to perform their tasks while appropriately addressing educational and business needs while 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):

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 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.
Requesting IT Assistance

PURPOSE

In order to assure prompt and efficient resolution of user requests the following procedures must be followed when requesting IT assistance. These policies are in place to ensure a consistent level of support.

STUDENTS

Students requesting technical assistance will be required to identify themselves based on the currently adopted Student Identification Policy. 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.
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 **Acceptable Use of Email**). 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.
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 staff or faculty, the Director of IT, or a member of University Administration.

INVESTIGATION

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

The Director of IT will obtain authorization from University Administration to monitor the user’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 and University Administration. Data gathered through monitoring will be kept confidential but will be made available to University Administration.

University Administration may inform the user 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 be subject to the violation and enforcement section of this policy. If a gross violation has occurred, University Administration will take appropriate action. Such action may result in losing access privileges, severe reprimand, dismissal and legal action which may include restitution for damages.
RELATED DOCUMENTS
Academic Honesty Policy

Email Best Practices

Student Laptop Lending Request Form