APPROPRIATE USE POLICY

Heartland Community College – Information Technology
Version 2.0 – 10/01/2013

Table of Contents

Source: https://share.heartland.edu/sites/workcenter/378/Series Documents/Policies/Appropriate Use Policy.docx
Publish: http://www.heartland.edu/policy/appropriateUsePolicy.pdf

Effective August 1, 2009, this policy replaces any prior policies related to technology resources and information.

1.0 INTRODUCTION

Heartland Community College (HCC) strives to remain a technologically forward institution. As such, the College is obligated to safeguard its technological infrastructure by establishing security and appropriate use guidelines for all users of HCC technology resources. The need for such a policy originates from access to both digital information and physical resources. Each member of the College community is afforded a level of access that is appropriate for the tasks he/she performs. Access is a privilege. It is accompanied by a responsibility to conduct activities within the parameters of this policy in an effective, ethical, and lawful manner. Policy violations will be addressed in accordance with Section 5.0 herein.

The misuse of any technology resource as described herein is not limited to the unauthorized or illegal use of that resource. Simply having access to a particular resource does not necessarily imply all usage of that resource is appropriate. Similarly, legality does not necessarily constitute appropriateness.

2.0 DEFINITIONS

Below is an alphabetical list of terms and their definitions as deemed appropriate for the purposes of this document.

2.1 Authentication

"Authentication" refers to the process a technology resource carries out in order to securely identify a user and verify that the user is who he or she claims to be. Authentication can occur in a number of ways with the most common method being a unique user name paired with a password. Other less common methods for authentication include biometric scans and smart cards with magnetic strips or bar codes.

2.2 Authorization

"Authorization" refers to the specific technology resources and the amount and type of information in each of those resources that a user is allowed to see and/or use. Authorization, also called "access", for each user is unique and is assigned based upon an individual's requirements for adequately, effectively, and efficiently performing the tasks of his or her official position.

2.3 Cloud Services

"Cloud Services" are services made available to users on demand via the Internet from a "cloud computing" provider's servers as opposed to being provided from an organization's own on-premises servers. Examples of cloud services would be Web-based e-mail services, hosted office suites and document collaboration services.

2.4 Cloud Storage

"Cloud Storage" is a service model in which data is maintained, managed and backed up remotely and made available to users over a network (typically the Internet).

2.5 IT

The abbreviation "IT" refers to the Information Technology Department and/or its members.

2.6 Individual Storage

"Individual Storage" refers to electronic file storage on a network drive that is named and reserved for use by one specific employee. Storage areas assigned to individual employees are used for storing files that are not typically needed by other College employees. Information

residing in individual storage is backed up by the College. While commonly referred to as "personal storage" or the "home directory," individual storage is considered to be property of the College, regardless of its content.

2.7 Information

"Information" refers to any data owned by the College. This includes any data stored on or used by any College-owned or College-licensed technology resource, and it includes any College related data such as student grades and IDs, even if that data were being stored on or used by equipment that is not College-owned. For example, in this document the term "information" may refer to student grades or other data being stored on personally-owned hardware such as digital assistants, laptops, home computers, and portable storage devices.

2.8 Login Name

"Login name" refers to a unique alphanumeric identifier that is assigned to each employee. Many technology resources at the College require employees to enter a login name and password in order to gain access to the resource. Once a user has authenticated using a login name and password, authorization to view and/or use specific information within the confines of the technology resource currently being accessed is granted based on the login information. For example, an employee who uses his or her login name and password to be admitted into the e-mail system will, upon entering the system, have access only to his or her specific mailbox and any authorized shared mailboxes.

2.9 Single Sign-On

"Single Sign-on" refers to the ability of a user to access multiple technology resources with one successful authentication to a primary account, which at HCC is a user's network account. For example, a successful sign-on to myHeartland also opens access to individual storage, IRIS, Blackboard, and email account without the need to re-enter a login name and password for every system.

2.10 System Administrator

"System Administrator" refers to certain employees in the IT department whose official positions at the College include duties related to network and telecommunication systems. These duties include, but are not limited to, troubleshooting and maintaining the College's network, setting up and maintaining user accounts, and assigning and monitoring file storage space such as individual, voice mail, and e-mail storage.

2.11 Technology Resource

"Technology Resource" refers to all College-owned or College-licensed electronic or digital hardware and software products or systems, including, but not limited to, the following:

- Network services (such as shared and personal file storage, Internet access, e-mail, and printing services)
- Mission critical systems (such as PeopleSoft, ImageNow, Compass, Blackboard)
- Telecommunication systems (such as telephone, cellular phone, voice mail, and fax systems)
- Desktop equipment (such as computers and peripherals in offices, classrooms, and common areas)
- Virtual machine
- Supplementary technology devices (such as scanners, digital cameras, video cameras, projectors, document cameras, TVs and VCRs, ITV systems, satellite, and public display systems)
- Mobile equipment (such as laptops and other personal computing devices)
- Retail software (such as Windows and Microsoft Office)

- Specialized applications (such as Peachtree, MathType, and Photoshop, as well as access to research databases such as FirstSearch)

Note: This list is representative. It cannot be exhaustive as technology resources at the College are constantly changing. This policy applies to all technology resources regardless of whether or not an individual item is specified in this list.

2.12 User

"User" refers to anyone who accesses or uses any College-owned or College-licensed technology resource. Such persons include, but are not limited to, students, employees, community members, vendors, contractors, and subcontractors. A personal network or other user account is not required to be considered a user. Also, neither the location of the user nor the location of the resource is of consequence. Persons accessing systems remotely, as is possible with Blackboard or library databases, are also considered users and are required to operate within the parameters of this policy.

2.13 User Account

"User account" refers to the information stored by a technology resource that identifies the user for authentication purposes. For example, the user account stores the password needed to authenticate a login name. Typically a user account also stores information on what resources a user has authorization to view and/or use within that particular system. For example, a user's network account allows access to the HCC network as well as specific drives on that network, and a Blackboard account allows access to an individual's specific online classes.

3.0 EMPLOYEE ACCESS TO TECHNOLOGY RESOURCES AND INFORMATION

Many technology resources at Heartland Community College require user authentication and authorization via a personal account. The rules and responsibilities described in this document apply to both network accounts and accounts in all other systems.

3.1 Eligibility for Access

All employees are eligible to receive a network account, e-mail account, and individual storage space on the network. Accounts that provide access to other systems such as PeopleSoft or ImageNow are granted based upon the responsibilities of the employee's official position and/or upon the request of the employee's supervisor. Supervisors may submit requests for changes to an employee's access rights to the IT department.

3.2 Sharing of System Accounts

Login names are non-transferable. A login name is to be used only by the employee to whom it is assigned. Similarly, passwords, by definition, are secret and may not be shared with any other person under any circumstances. Allowing another individual to use a login name and password, either knowingly or negligently, is a violation of the appropriate use policy. Policy violations will be addressed in accordance with Section 5.0 herein.
Note: Employees who request assistance from IT while using the login name and password of another user will be denied assistance. Additionally, violation of the appropriate use policy will be documented and reported to the Director of Technology Support Services.

3.3 Position Changes

Reassignment of authorizations resulting from internal employment changes are managed on a case-by-case basis. If an employee moves to a different department, his or her login name and e-mail address will remain the same. However, all other access that was originally granted based on the duties of the employee's prior position will be suspended.

It is the responsibility of the employee's new supervisor to submit a new request for authorizations appropriate to the new job duties.

3.4 Disabling User Accounts

A request to disable account access to College technology resources may be put forth by an employee's supervisor, the Executive Director of Human Resources, or a member of the Cabinet. Such requests will be carried out by a College system administrator. Also, a system administrator, at his or her own discretion, may disable an employee's account in order to protect the integrity of the College network.

Upon notification from Human Resources, the account of a terminated employee will have its authorization reduced to that of a student account.

4.0 APPROPRIATE USE OF TECHNOLOGY RESOURCES

Information technology plays an integral role in allowing employees to accomplish their assigned duties. There is an ever-growing array of computing services that empowers employees to create, access, evaluate, update, distribute, store, and report on information using a variety of media and formats. Understanding that a College employee may be severely hindered in the ability to perform his or her duties if he or she lacks access to appropriate technology resources, Heartland Community College provides such resources in support of the various activities of the institution. These resources are intended for the sole use of Heartland employees, students, and other authorized users. The use of these technology resources is a privilege and demands individual responsibility for security and appropriateness.

It is impossible to identify every situation that pertains to proper or improper use of technology resources. The list below describes some general guidelines regarding prohibited activities, and focuses on some of the more significant responsibilities an employee accepts when he or she chooses to use a College-owned or College-licensed technology resource.

4.1 General Restrictions

Use of technology resources shall be within the spirit or principles of this policy. No one shall attempt to circumvent or undermine the intent of this policy. Discovering and operating within a loophole of the policy constitutes unacceptable behavior and will be considered a policy violation. Policy violations will be addressed in accordance with Section 5.0 herein.

4.2 Other Applicable College Policies

Many information technology functions parallel similar activity in other formats making existing College policies important in determining what use is appropriate. For example, the College's copyright policy applies not only to hard-copy documents, but also to electronic documents. Also, the College's harassment policy applies not only to face-to- face harassment, but to harassment via electronic means as well. For statements defining other applicable College policies, consult the Employee Handbook.

4.3 Physical Misuse of Resources

General physical misuse of technology resources such as any unauthorized loan, unauthorized removal of equipment from campus, theft, damage, or destruction is strictly prohibited.

4.4 Use of Resources and Information for Profit

Using Heartland Community College technology resources for commercial purposes including, but not limited to, the promotion or day-to-day operation of "for profit" and/or

privately-owned businesses or commercial ventures is strictly prohibited. This includes any use of College-owned information or equipment for solicitation purposes.

4.5 Software

4.5.1 Software Licensing

It is the responsibility of the IT department to ensure that the College remains in legal compliance with all software licenses, subscriptions, and contractual agreements regardless of the budget from which a software resource was funded. Consequently, IT is responsible for storing and maintaining application software, as well as for understanding and ensuring College compliance with software license agreements.

4.5.2 Software Application Availability

All College computers are equipped with a set of standard software applications including, but not limited to, programs such as Microsoft Windows, Microsoft Office, and Internet Explorer.

Additional applications may be available upon request. Procedures for requesting additional applications are maintained within IT.

4.5.3 Software Installation/Removal

The IT department is responsible for installing and removing all software applications. Employees are prohibited from loading applications or utilities on any physical workstation or virtual machine unless given specific authorization from IT. Similarly, employees are prohibited from removing applications or utilities from a workstation without IT authorization. The IT department retains the right to remove any personal or other non-College-owned applications downloaded from the Internet or otherwise installed on a workstation, regardless of whether or not previous authorization was granted. Removal of software may be necessary in a variety of situations such as restoring functionality of College systems, resolving policy violations, or ensuring compliance with licensing requirements.

4.5.4 Software Reproduction

Reproduction or duplication of College-owned or College-licensed software using any type of media or through any type of electronic transmission without prior authorization from IT is prohibited.

4.6 Hardware

4.6.1 Hardware Installation/Removal

The IT department is responsible for acquiring, installing, moving, and removing all hardware devices in all campus common areas such as classrooms, computer labs, and office areas.

In assigned office spaces, employees outside of the IT department may only connect or disconnect hardware devices with prior authorization from IT. Authorization for many peripheral devices such as mice and keyboards can be obtained by calling the IT hotline. Personal devices connected to College resources must be identified as such, preferably with a label identifying the owner. Whether or not authorization was originally granted, the IT department retains the right to disconnect any personally-owned equipment connected to College resources.

4.6.2 Standard Media Device Use

Employees may use College-owned or personal media and memory devices such as diskettes, USB drives, CD-ROMs, etc. with any College-owned equipment without prior authorization from IT. However, these devices may not be used to copy, transfer, or remove sensitive or protected information from College-owned or College-licensed technology resources unless such activity is authorized by the employee's supervisor. Employees should never store confidential and sensitive information on personal media or portable storage devices such as USB drives or smart phones. These devices can be easily stolen or misplaced leaving the College vulnerable to a security breach.

4.7 Electronic Communications

The following policy guidelines apply to all forms of electronic communication used by College employees when communicating using College-owned or College-licensed technology resources. Electronic communication methods include, but are not limited to, phones, voice mail messages, e-mails, instant messaging, online newsgroups, faxes, radios, and College-owned cell phones. Except as otherwise excluded by law or collective bargaining language, all devices, files, messages and storage associated with such electronic communications are the property of the College regardless of their content.

Note: The College recognizes issues surrounding intellectual property rights and will make every effort to respect the rights of the individual. In situations where ownership of content is in question, the College will abide by the law and established legal precedence with regard to those issues.

4.7.1 Responsibilities

The e-mail system is the primary means by which College information is disseminated. All employees are required to check their e-mail for distribution of such messages at least one time per week unless on an official leave.

4.7.2 Requirements

A general e-mail confidentiality notice is automatically appended to all e-mail messages sent via the College's e-mail system. This notice identifies Heartland Community College as the owner of the information and provides instructions for recipients who have received a message in error. Employees may not block, hide, or cancel this notice.

4.7.3 Restrictions

Etiquette commonly used for traditional written communications should be used as a guideline for electronic communications. Every employee should be continually aware that he or she represents Heartland Community College with every communication he or she sends. Inappropriate communications are prohibited. Instances of inappropriate electronic communications include, but are not limited to, the following:

4.7.3.1 Fraudulent Communications

Any electronic communication sent under an assumed name or modified address, or with the intent to obscure the origin, date, or time of the communication is considered fraudulent and is prohibited.

4.7.3.2 Harassing Communications

Any electronic communication that constitutes harassment as defined by the Heartland Community College harassment policy is prohibited.

4.7.3.3 Mass Communications

Employees may not knowingly create or send unapproved communications that will generate excessive network traffic. Examples of this type of communication include chain letters, unwelcome e-mails, e-mail bombs, viruses, hoaxes, and/or other mass communications that may potentially degrade the performance of the network infrastructure.

4.7.3.4 Confidential Personnel Communications

In keeping with the College's policies and collective bargaining agreements, disciplinary activities are to take place in-person between a supervisor and his or her subordinate. Employees are prohibited from using direct e-mail communications and/or voice mail to address confidential disciplinary issues with other employees. Similarly, employees are asked to refrain from criticizing others using e-mail and/or voice mail. The e-mail system may be used to transmit files or documentation related to disciplinary activity as long as such files are sent as attachments and the original files or documentation are stored elsewhere (i.e., the information should not exist solely in the e-mail system).

Note: Due to the confidential nature of such communications, employees are encouraged to submit claims of harassment or other policy violations using methods other than e-mail. However, if such a claim is submitted via the e-mail system, the claim will be addressed, regardless of the method of communication.

4.7.3.5 Copyright

Electronic communications are prohibited from including any information that violates the College's copyright policy or any state or federal copyright law.

4.8 Internet Use

Information available via the Internet may be distracting, objectionable, or even disturbing. Since many technology resources may be visible and/or audible to others, sensitivity in viewing and/or listening to such material is required. Users who disturb or distract others may be asked to stop their activities or leave a particular area.

4.8.1 Downloading/Uploading

Downloading is when data is transferred from a main source to a device such as a desktop computer. Conversely, uploading is when data is transferred from a device such as a desktop computer to a main source such as a server. Using College-owned resources to download or upload copyrighted material outside of Fair Use rules without obtaining a copyright release is prohibited. Copyrighted material may include, but is not limited to, audio files, graphics, video files, and electronic publications.

4.8.2 Peer-to-Peer File Sharing

Peer-to-peer (P2P) file sharing occurs when files stored on one computer are sent directly to another computer across the Internet. In a P2P network, each computer functions as a client and a server, with each having equal privileges to download and/or upload files to other computers on the network. Although P2P file sharing is legal; sharing, distributing, or downloading copyrighted material typically is not.

College-owned technology resources may not be used in a P2P network to illegally transfer copyrighted materials. Further, P2P software shall not be installed on any college owned computer in accordance with section 4.5.3 herein.

4.8.3 Pornography

Employees are prohibited from using College-owned or College-licensed technology resources for accessing images, sounds, or messages that are pornographic in purpose. Legal, sexually explicit literary/artistic expressions and materials that are relevant and appropriately related to course subject matter or curriculum are not considered to be pornographic in purpose.

4.9 Network Bandwidth Use

Large-scale distribution of such things as MP3 music or video files or the use of streaming audio or video can cause excessive network loading that may cause a significant decrease in network performance and affect all users. Therefore, no one may knowingly or recklessly download or distribute such data, digital audio or video files, or audio or video streams. Employees who believe they need to perform these types of actions within the confines of their job responsibilities must contact IT for assistance in completing the task in a manner that will not negatively impact other users.

4.10 Duplication/Reproduction of Copyrighted Materials

Typically, copyrights belong to the original author(s) of a work, regardless of whether a work is published or unpublished. In general, a copyright release is required to legally duplicate or otherwise reproduce copyrighted material. This requirement pertains to all works regardless of the medium on which the work is stored. Some examples of storage media used at Heartland Community College that may contain copyrighted material are VHS and 8mm tapes, CDs, DVDs, diskettes, zip disks, and USB devices.

4.10.1 IT Duplication Requests

Requests submitted to IT for duplication of files from one medium to another will be individually evaluated and granted only when the request is acceptable within the confines of the College's copyright policy. For example, at the request of the recording instructor, it is appropriate for IT to copy recordings of classroom presentations from 8mm tapes to VHS tapes to facilitate future viewing of such recordings.

4.10.2 Duplication/Reproduction of College-Owned Information

Duplication and/or reproduction of College-owned copyrighted material in any form without proper authorization and release is prohibited. Neither authorization nor release will be granted for requests that are not in accordance with the College's copyright regulations or that go against federal or state law.

4.10.3 Duplication/Reproduction of Personally-Owned Information

College-owned technology resources, including media, may not be used for the duplication and/or reproduction of personally-owned copyrighted material (i.e., simply having purchased a music CD or movie DVD does not give the purchaser any legal right to copy it).

4.10.4 TEACH

The Technology, Education, and Copyright Harmonization Act, also known as the TEACH Act, was created to allow distance education instructors and students to take advantage of the copyright exceptions granted to classroom educators under the doctrine of Fair Use. There are some differences in how copyrighted material may be used in a classroom versus in distant learning situations. Employees who wish to take advantage of the allowances provided by the TEACH Act to transmit copyrighted materials to online course participants must contact IT for assistance in technologically enforcing the regulations specified in the TEACH Act.

For more information about the provisions of the TEACH Act and Fair Use, consult with the Director of Library and Information Services.

4.11 Personal Use

Limited, reasonable personal use of College resources is permissible. However, such use cannot interfere with the employment responsibilities of the employee, must comply with the guidelines established herein, and is conducted at the employee's own risk, without an expectation of privacy.

4.12 Cloud Storage of College Information

There are many cloud storage services available such as Dropbox, Google Drive, and Microsoft SkyDrive. Many offer a free service with limited data storage to individual users. These services offer a convenient file storage solution that allows access to files from virtually anywhere and have subsequently become very popular. However, these third party services are not appropriate for the storage of all types of files. It is important to realize that these providers may change how they handle things such as privacy, security, and file ownership. While these organizations are diligent at securing information, it is possible for their security to be breached.

Heartland Community College prohibits employees from using third party cloud storage service providers to store any files containing Confidential and Sensitive Information (CSI) as defined in section 4.0 of the Heartland Community College Information Security Policy.

4.13 Bring Your Own Device

Bring Your Own Device (BYOD) is a phrase used to describe a type of computing where employees, students, and others bring their own mobile device (notebook, tablet, smartphone, etc.) and use it in the College's computing environment. BYOD brings many advantages and challenges to an organization. One challenge is security management. Heartland Community College requires any user that will use a personal device to access College resources (e-mail, virtual desktops, etc.) to secure their device with a password enabled screen lock.

4.14 Upholding the Mission

College technology resources shall not be used in any manner that violates or conflicts with the College's mission and/or its policies.

5.0 CONSEQUENCES FOR POLICY VIOLATIONS

Heartland Community College considers any violation of appropriate use guidelines to be a serious offense. Violators of this policy will be subject to disciplinary action in accordance with the College's progressive discipline policy, up to and including discharge. In addition to College discipline, violators of this policy may be subject to criminal prosecution, civil liability, or both for unlawful use of any technology resource.

6.0 POLICY DEVELOPMENT AND MAINTENANCE

This policy document is available to all employees. Employees may access the document via the College's public drive or may request a printed copy from the Information Technology Department or the Human Resources Department.

This policy will be reviewed periodically as determined by the Chief Information Officer. Concerns or questions about the policy may be directed to the Director of Technology Support Services, the Chief Information Officer, or the Vice President of Business Services.