APPROPRIATE USE POLICY

Heartland Community College – Information Technology
Version 3.0 – 06/12/2019

Table of Contents

Effective June 12, 2019, this policy replaces any prior policies related to technology resources and information.

1.0 PURPOSE

Heartland Community College (HCC) strives to remain a technologically forward institution. As such, the HCC 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 HCC community is afforded a level of access that is appropriate for the tasks he/she performs. Access is a privilege. As a user of these services and facilities, you have access to valuable HCC resources, to sensitive data, and to internal and external networks. 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 12.0 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 SCOPE

This policy applies to all users of computing resources owned or managed by HCC. Individuals covered by the policy include (but are not limited to) HCC faculty and visiting faculty, staff, temporary employees, contractors, consultants, students, alumni, agents of the administration, external individuals guests such as volunteers, and other members of the HCC community, including those affiliated with third parties, who access or in any way make use of HCC information or information systems; and accessing network services via HCC computing facilities.

Computing resources include all HCC owned, licensed, or managed hardware and software, and use of the HCC network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

“Information resources” include information in any form and recorded on any media, and all computer hardware, computer software, and communications networks owned or operated by HCC or on behalf of HCC; and any device, regardless of ownership and including equipment privately owned by faculty, staff, and students (e.g., laptop computers, tablet computers, smart phones, MP3 players, USB storage devices, etc.), but only with respect to the ways in which they connect to or access HCC information resources and the activities they perform with those resources.

These policies apply to technology and resources administered by various HCC departments, personally owned computers and devices connected by wire or wireless to the campus network, and to off-campus computers that connect remotely to HCC network services.

3.0 YOUR RIGHTS AND RESPONSIBILITIES

As a member of the HCC community, HCC provides you with the use of scholarly and/or work-related tools, including access to the Library, to certain computer systems, servers, software and databases, to the campus telephone and voice mail systems, and to the Internet. You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether you are an HCC employee or a matriculated student), and of protection from abuse and intrusion by others sharing these resources. You can expect your right to access information and to express your opinion to be protected as it is for paper and other forms of non-electronic communication.

In turn, you are responsible for knowing the regulations and policies of HCC that apply to appropriate use of HCC technologies and resources. You are responsible for exercising good judgment in the use of HCC technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.
As a representative of the HCC community, you are expected to respect the good name of HCC in your electronic dealings with those outside of HCC.

3.1 Guest Access

Access to the campus network by a guest shall be coordinated through an HCC sponsor. The sponsor will take responsibility for the actions of the guest while they are using resources. Staff or faculty at service desks (library reference desk, computer help desk, or event support staff) shall not generally sponsor guests unless they have invited the guest to campus or are asked to sponsor the guest by an eligible sponsor.

4.0 POLICY

4.1 Appropriate use

You may use only the computers, computer accounts, and computer files for which you have authorization.

You may not use another individual's account, or attempt to capture or guess other users' passwords.

You are individually responsible for appropriate use of all resources assigned to you, including the computer, the network address or port, software and hardware. Therefore, you are accountable to HCC for all use of such resources. As an HCC authorized user of resources, you may not enable unauthorized users to access the network by using an HCC computer or a personal computer that is connected to the HCC network.

HCC is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.
You should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access. You must configure hardware and software in a way that reasonably prevents unauthorized users from accessing the HCC network and computing resources.
You must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.

You must comply with the policies and guidelines for any specific set of resources to which you have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

You must not use HCC computing and/or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.

On the HCC network and/or computing systems, do not use tools that are normally used to assess security or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless you have been specifically authorized to do so by the Information Technology department.

5.0 DEFINITIONS

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

5.1 Appropriate use

“Appropriate use” means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Appropriate Use Policy, HCC will take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from HCC. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. These policies and laws are subject to change as state and federal laws develop and change.

5.2 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.

5.3 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.

5.4 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.

5.5 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).

5.6 IT

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

5.7 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 HCC employees. Information residing in individual storage is backed up by HCC. While commonly referred to as “personal storage” or the “home directory,” individual storage is considered to be property of HCC, regardless of its content.

5.8 Information

“Information” refers to any data owned by HCC. This includes any data stored on or used by any HCC-owned or HCC-licensed technology resource, and it includes any HCC related data such as student grades and IDs, even if that data were being stored on or used by equipment that is not HCC-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.

5.9 Login Name

“Login name” refers to a unique alphanumeric identifier that is assigned to each employee. Many technology resources at HCC 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.

5.10 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, Canvas, and e-mail account without the need to re-enter a login name and password for every system.

5.11 System Administrator

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

5.12 Technology Resource

“Technology Resource” refers to all HCC-owned or HCC-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, Canvas)
- 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 DVD players, 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 HCC are constantly changing. This policy applies to all technology resources regardless of whether or not an individual item is specified in this list.

5.13 User

"User" refers to anyone who accesses or uses any HCC-owned or HCC-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 Canvas or library databases, are also considered users and are required to operate within the parameters of this policy.

5.14 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 Canvas account allows access to an individual's specific online classes.

6.0 EMPLOYEE ACCESS TO TECHNOLOGY RESOURCES AND INFORMATION

Many technology resources at HCC 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.

6.1 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.

6.2 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 12.0 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 IT Help Desk.

6.3 Institutional Need for Access to Confidential or Restricted Information

Confidential or restricted information concerning individual students or employees may be viewed when there is an institutional need or this information is needed based on specific job duties or the individual's job description. It is recognized that a small number of areas, departments, and processes at HCC will qualify for access to confidential or restricted information. There are specific responsibilities and guidelines within the respective department or division that are to be followed when the individual collects, stores, or uses this confidential information at HCC. Employees have an implied stewardship of responsibility when working with confidential information.

6.4 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.

6.5 Disabling User Accounts

A request to disable account access to HCC 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 an HCC 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 HCC network.

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

7.0 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 an HCC employee may be severely hindered in the ability to perform his or her duties if he or she lacks access to appropriate technology resources, HCC provides such resources in support of the various activities of the institution. These resources are intended for the sole use of HCC employees, students, and other authorized users. The use of these technology resources is a privilege and demands and accepts individual responsibility for security and appropriateness.

7.1 Other Applicable HCC Policies

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

7.2 Hardware

7.2.1 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 Help Desk. Personal devices connected to HCC 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 HCC resources.

7.2.2 Standard Media Device Use

Employees may use HCC-owned or personal media and memory devices such as diskettes, USB drives, CD-ROMs, etc. with any HCC-owned equipment without prior authorization from IT. However, these devices may not be used to copy, transfer, or remove sensitive or protected information from HCC-owned or HCC-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 HCC vulnerable to a security breach.

7.3 Electronic Communications

The following policy guidelines apply to all forms of electronic communication used by HCC employees when communicating using HCC-owned or HCC-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 HCC-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 HCC regardless of their content.

Note: HCC 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, HCC will abide by the law and established legal precedence with regard to those issues.

7.3.1 Responsibilities

The e-mail system is the primary means by which HCC 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.

7.3.2 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 HCC with every communication he or she sends.

8.0 PROHIBITED AND INAPPROPRIATE USE

Users of HCC information resources are prohibited from engaging in any activity that is illegal under local, state, federal, or international law or in violation of HCC policy. The categories and lists in the sections that follow are not exhaustive, but provide a framework for activities that fall into the category of prohibited and inappropriate use.

8.1 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 inappropriate behavior and will be considered a policy violation.

8.2 Excessive Non-Priority Use of Information Resources

Priority for the use of information resources is given to activities related to HCC academic, research, and public service mission. To conserve resource capacity for all users, individuals should exercise restraint when utilizing computing and network resources. Individual users may be required to halt or curtail non-priority use of information resources, such as recreational activities and nonacademic, non-business services.

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

8.3 Inappropriate System and Network Activities

Inappropriate system and network activities include:

<u>8.3.1 Security Breaches or Malicious Use</u>

Engaging in or effecting security breaches or malicious use of network communication including, but not limited to:

8.3.1.1 Obtaining Unauthorized Configuration Information

Obtaining configuration information about a network or system for which the user does not have administrative responsibility.

8.3.1.2 Increase Network Traffic or Create Nuisance Traffic

Engaging in activities intended to hide the user’s identity, to purposely increase network traffic, or other activities that purposely endanger or create nuisance traffic for the network or systems attached to the network.

8.3.1.3 Develop or Use Mechanism To Alter Or Avoid Charges

Attempting to develop or use any mechanism to alter or avoid charges levied by HCC for information resources (e.g., printing).

8.3.1.4 Intercept Network Communications

Attempting to intercept network communications for purposes of rerouting packets, forging packets, packet “sniffing,” or reading message/file content.

8.3.1.5 Scanning Network For Systems To Take Advantage Of Vulnerabilities

Scanning HCC networks or systems for security vulnerabilities (this includes port scanning).

8.3.1.6 VPN Software or Anonymizing Software

Using unauthorized VPN or other anonymizing software to or from campus network or desktops.

<u>8.3.2 Modifying Configuration of Computing Infrastructure</u>

Modifying the configuration of HCC computing infrastructure in any way including, but not limited to:

8.3.2.1 Adding or removing network links, wireless access points, wireless routers, switches, computers, circuit boards, or peripherals (e.g., disks, printers, modems, cameras, etc.).

8.3.2.2 Reconfiguring the HCC network addressing structure in any way. HCC is the sole provider of network services such as Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), and routing on HCC networks; any computer or equipment that replicates or disrupts these services will be immediately disconnected.

8.3.2.3 (Re)installing operating systems or changing base configurations on HCC-owned or –operated systems.

8.3.2.4 Reconfiguring any control switches or parameters.

8.3.3 Circumvent User Authentication and Unauthorized Access

Circumventing or attempting to circumvent user authentication and access control mechanisms; accessing or altering data, accounts, or systems that the user is not expressly authorized to access.

8.3.4 Interfere With Another User or Persons Service or HCC Network

Interfering with or denying service to another user on the campus network or using HCC facilities or networks to interfere with or deny service to persons outside HCC.

8.3.5 Unauthorized Installation of Monitoring Device

Installing any monitoring device, whether physical or electronic, that attempts to monitor or record the movement or activity of members of the HCC community. This includes, but is not limited to the unauthorized installation of webcams for any monitoring purpose within HCC, or the use of cell phone cameras for this purpose.

8.4 Unauthorized Use of Intellectual Property

Users may not use HCC information resources to violate the ethical and legal rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations. Violations include, but are not limited to:

8.4.1 Copyright

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

8.4.1.1 Unauthorized Use of Copyrighted Material

Except as provided by fair use principles, engaging in unauthorized copying, distribution, display, or publishing of copyrighted material including, but not limited to:

8.4.1.1.1 Digitization and distribution of photographs from magazines, books, or other copyrighted sources,

8.4.1.1.2 Distribution of copyrighted music or video, and

8.4.1.1.3 Installation of any copyrighted software without an appropriate license.

8.4.1.2 Inappropriate Peer-To-Peer File Sharing

Using peer-to-peer file sharing programs or file sharing web sites to upload or download protected intellectual property such as copyrighted music or video or illicit copies of licensed software (“warez”).

8.4.2 Unauthorized Use of Trademarks and Logos

Using, displaying, or publishing licensed trademarks, including HCC trademarks, without license or authorization or using them in a manner inconsistent with terms of authorization. Use of HCC trademarks and logos must comply with the policies and guidelines published by the Marketing Department.

8.4.3 Exporting Software or Technology Violation

Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws.

8.4.4 Confidentiality Breach

Breaching confidentiality agreements or disclosing trade secrets or pre-publication research.

8.4.5 Academic Dishonesty and Plagiarism

Using computing facilities and networks to engage in academic dishonesty prohibited by HCC policy (such as unauthorized sharing of academic work or plagiarism).

8.5 Inappropriate or Malicious Use of IT Systems

8.5.1 Introducing Malicious Programs into Network or Computer Systems

Intentionally introducing malicious programs into the network or computer systems (e.g., viruses, worms, Trojan horses, spyware, e-mail bombs, etc.).

8.5.2 Granting Access to Non-Authorized Users

Granting any form of information resource access to non-authorized users. This includes, but is not limited to, giving electronic library access to non-authorized persons or any other attempt to give benefit or privilege of HCC information resources to a nonauthorized person.

8.5.3 Intercept, Compromise or Tamper with User Passwords

Attempting to intercept, compromise, or tamper with user passwords. This includes, but is not limited to, copying passwords files, password “cracking,” installing keystroke logging software, intercepting network traffic, or otherwise attempting to discover passwords belonging to other individuals. It also includes taking advantage of another user’s naiveté to gain access to information resources, or preventing someone from using his or her account by changing the password or through other tampering.

8.5.4 Displaying, Procuring or Transmitting Material in Violation of Code of Conduct

Using an HCC information resource to actively engage in displaying, procuring, or transmitting material that is in violation of HCC codes of conduct, sexual or discriminatory harassment policies or laws, hostile workplace laws, or other illegal activity.

8.6 Misuse of E-Mail and Communications Activities

Electronic mail (e-mail) and communications are essential in carrying out the activities of HCC and to individual communication among faculty, staff, students, and their correspondents. Some key prohibitions include:

8.6.1 Tampering with Email Confidentiality Notice

A general e-mail confidentiality notice is automatically appended to all e-mail messages sent via the HCC e-mail system. This notice identifies HCC 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.

8.6.1.1 Harassing Communications

Any electronic communication that constitutes harassment as defined by the HCC harassment policy is prohibited.

8.6.1.1.1 Engaging in harassment via e-mail, telephone, paging, texting, or social media, whether through language, frequency, or size of messages.

8.6.1.2 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.

8.6.1.2.1 Masquerading as someone else by using their e-mail or Internet address or electronic signature, or altering the content of a message from another person with intent to deceive.

8.6.1.2.2 Soliciting e-mail from any other e-mail address, other than that of the poster's account, with the intent to harass or collect replies.

8.6.1.2.3 Forwarding or otherwise distributing information obtained from another individual that the individual reasonably expects to be kept confidential.

8.6.1.3 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, quick-profit schemes, and/or other mass communications that may potentially degrade the performance of the network infrastructure.

8.6.1.3.1 Using e-mail originating from within HCC networks and e-mail systems for commercial purposes or personal gain.

8.6.1.3.2 Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material, except as approved by the Marketing Department or Student Support Services.

8.7 Use of Resources and Information for Profit

Using HCC 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 HCC-owned information or equipment for solicitation purposes.

8.8 Unauthorized Use of Software

8.8.1 Software Licensing

It is the responsibility of the IT department to ensure that HCC 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 HCC compliance with software license agreements.

8.8.2 Software Application Availability

All HCC 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.

8.8.3 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-HCC-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 HCC systems, resolving policy violations, or ensuring compliance with licensing requirements.

8.8.4 Software Reproduction

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

8.8.4.1 Confidential Personnel Communications

In keeping with the HCC 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.

8.9 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.

8.9.1 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 HCC-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.

8.9.2 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.

HCC-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 HCC-owned computer in accordance with section 4.5.3 herein.

8.9.3 Pornography

Employees are prohibited from using HCC-owned or HCC-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.

8.10 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.

8.11 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 HCC that may contain copyrighted material are CDs, DVDs, diskettes, zip disks, and USB devices.

8.11.1 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 HCC copyright policy.

8.11.2 Duplication/Reproduction of HCC-Owned Information

Duplication and/or reproduction of HCC-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 HCC copyright regulations or that go against federal or state law.

8.11.3 Duplication/Reproduction of Personally-Owned Information

HCC-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).

8.11.4 TEACH Act

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.

8.12 Personal Use

Limited, reasonable personal use of HCC 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.

8.13 Cloud Storage of HCC Information

8.13.1 Personally Acquired Cloud Resources

There are many cloud storage services available such as Dropbox, Google Drive, and Microsoft OneDrive. 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.

8.13.2 HCC Provided Cloud Resources

HCC provides employees with cloud based services such as Office365, Outlook, Teams, SharePoint along with a number of cloud based department specific applications such as Accommodate, Raiser’s Edge, etc. to perform operations on behalf of HCC. Many of these types of cloud resources provide easy access to content from personal or public devices. HCC employees are responsible as stewards of the information they work with, including and especially so regarding Confidential and Sensitive Information (CSI). Employees using these HCC provided resources are responsible to be sure no information is left on public devices. Employees should also not allow confidential or sensitive materials to be left on their personal devices as they are not secured by HCC and do not meet HCC security standards and practices for maintenance.

HCC prohibits employees from using third party cloud storage service providers to store any files containing Confidential and Sensitive Information (CSI).

8.14 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 HCC computing environment. BYOD brings many advantages and challenges to an organization. One challenge is security management. HCC requires any user that will use a personal device to access HCC resources (e-mail, virtual desktops, etc.) to secure their device with a password enabled screen lock.

8.15 Upholding the Mission

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

9.0 COMPLIANCE

Compliance with this Policy is mandatory for all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers, and other members of the HCC community, including those affiliated with third parties, who access or in any way make use of HCC information or information systems.

10.0 MONITORING

HCC considers the data processed by and stored on administrative computer systems to be the property of the HCC. The contents of user accounts are considered to be the property of the authorized user, subject to applicable HCC copyright and intellectual property policies and applicable federal and state laws. Examples of applicable laws, rules and policies include:

- The U.S. Electronic Communications Privacy Act, U.S. Computer Fraud and Abuse Act, and Article 156 of the New York Penal Code, which prohibit “hacking,” “cracking,” and similar activities;
- Laws governing libel, privacy, copyright, trademark, obscenity and child pornography;
- HCC Sexual Harassment Policy and Discriminatory Harassment Policy;
- HCC Student Code of Conduct and Employee Code of Conduct
- The Family Educational Rights and Privacy Act (FERPA) governs what information about students may be considered public and what information must be protected, and students’ rights with respect to that information.
- The Gramm-Leach-Bliley Act of 1999 (GLBA) requires organizations that provide financial services (e.g., student loans) to protect the security and confidentiality of individuals’ personally identifiable financial information.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects the privacy of health information created, transmitted, or maintained by health care providers and other institutions by electronic means. The services provided by Student Health and Support Services do not qualify HCC as a “covered entity” under HIPAA; however, information collected in the provision of these services is subject to protection under FERPA.

Individuals should be aware that their use of HCC information resources, including accessing the Internet or using electronic mail, social media, instant messaging, telephone, or voice mail, are not completely private. While HCC does not routinely monitor individual usage of its information resources, the normal operation and maintenance of these resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service. HCC may also specifically monitor the activity and accounts of individual users of HCC information resources, including individual login sessions, the content of individual communications, and the contents of stored information, with or without notice, when:

- The individual has voluntarily made the information accessible to the public, as by posting to a blog or a Web page;
- it reasonably appears necessary to do so to protect the integrity, security, or functionality of HCC information resources or to protect HCC from liability;
- a written complaint has been received, or there is reasonable cause to believe, that the individual has violated or is violating this policy;
- an account appears to be engaged in unusual or unusually excessive activity; or
- it is otherwise required or permitted by law.

Any such monitoring of communications or stored information, other than what is made accessible by the individual, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the Chief Information Officer, the Executive Director for Human Resources, the Dean for Student Support Services, or the Director of Network and System Administration, as appropriate. HCC, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications or stored information, to appropriate HCC personnel or law enforcement agencies and may use those results in appropriate HCC disciplinary proceedings.

11.0 REPORTING SECURITY INCIDENTS

Effective security response includes the prompt and appropriate response to breaches in security. It is incumbent on all individuals to report incidents in which they believe the security or privacy of HCC information resources has been jeopardized. Individuals are responsible for reporting security incidents to the Information Technology Helpdesk and/or the applicable Helpdesk with other affiliated Third Party software applications, and for taking action as recommended or directed by those authorities. Suspected violations must be reported to the IT Help Desk at 309-268-8350 or by email at helpdesk@heartland.edu.

12.0 CONSEQUENCES FOR POLICY VIOLATIONS

HCC 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 HCC progressive discipline policy, up to and including discharge. In addition to HCC discipline, violators of this policy may be subject to criminal prosecution, civil liability, or both for unlawful use of any technology resource.

In the case of a written complaint of serious misuse, or evidence indicating that malicious software may be present in certain material on the system, HCC reserves the right to temporarily remove material from the system for its review. In some situations, it may also be necessary to restrict or suspend access or account privileges to prevent ongoing misuse while the situation is under investigation.

Alleged infractions of this policy are handled via formal procedures and investigation by the Chief Information Officer, the Executive Director for Human Resources, the Dean for Student Support Services, or the Director of Network and System Administration, as appropriate. Upon determination of misuse, individuals who are found to be in violation of this Policy may be subject to the following:

- Restriction or suspension of computer access privileges;
- Disciplinary action by their department and/or HCC up to and including termination;
- Referral to law enforcement authorities for criminal prosecution;
- Third parties, including vendors and guests, in violation of HCC Policies may be subject to reduced service or denied service, or otherwise restricted in their ability to conduct business with HCC.
- Students found to be in violation of this policy may be subject to discipline in accordance with the HCC Student Handbook; and
- Other legal action, including action to recover civil damages and penalties.

13.0 POLICY DEVELOPMENT AND MAINTENANCE

This policy document is available to all employees. Employees may access the document via the HCC 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 IT Help Desk, the Chief Information Officer, or the Vice President of Business Services.