

Heartland Community College
APPROPRIATE USE POLICY FOR STUDENTS & COMMUNITY USERS

Effective 8/21/2006: this policy replaces any prior policies related to technology resources and information.

1.0 INTRODUCTION

The purpose of this appropriate use policy is to safeguard the technological infrastructure of the institution by establishing appropriate use guidelines for all rightful users of technology resources. The primary goal of this policy is to prevent problems before they occur.

Heartland Community College provides students and community members with a wide array of technology resources. Access to these resources 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. Violators of this policy may have access revoked and/or be subject to disciplinary action in accordance with the institution’s student conduct policy.

2.0 DEFINITIONS

2.1 Technology Resources

This policy frequently refers to “technology resources.” At Heartland Community College this term encompasses many components, including but not limited to:

- network services (such as Internet access and printing services);
- all mission critical systems (such as IRIS and WebCT);
- physical equipment including computers and peripherals in all classrooms, and common areas (labs, library, etc.);
- all supplementary technology devices (such as scanners, digital cameras, video cameras, projectors, document cameras, TVs and VCRs, ITV systems, and satellite systems)
- all retail software and all specialized academic applications (such as Peachtree or Mathtype).

The policy applies to all technology resources regardless of whether or not an individual item is included in this list.

2.2 User

The term “user” refers to anyone who utilizes any technology resource owned by Heartland Community College, regardless of the location of the resource or the user. In other words, a user will be required to operate within the parameters of this policy whether he or she is using systems on-site or remotely, such as is possible with WebCT or library databases.

2.3 Information Technology (IT)

“IT” refers to the Information Technology Department within the Business Services division. NOTE: There is an academic Technology department within the Instructional Services division of the college.

3.0 APPROPRIATE USE OF TECHNOLOGY RESOURCES

It is not the intent of this policy to identify every situation that pertains to proper or improper use of technology resources. The list below focuses on some of the most significant responsibilities a user accepts when he or she chooses to use a College-owned technology resource, as well as general guidelines regarding prohibited activities.

3.1 General Restrictions

The 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 relating to the use of technology resources. Discovering and operating within a loophole of the policy may constitute inappropriate use.

3.2 Other Applicable College Policies

The Policy may be viewed at: www.heartland.edu/policy/appropriateUseAtHeartland.pdf

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 Copyright Policy applies not only to hard-copy documents, but to electronic documents as well. Using a technology resource in order to violate any college policy constitutes inappropriate use. For review of other applicable college policies, such as the Information Privacy Policy, please consult the Heartland Community College Catalog or the Heartland Community College web site.

3.3 Software

3.3.1 Software Installation and Licensing

The IT Department ensures that the College remains in legal compliance with all software licenses, subscriptions, and contractual agreements. Students may download software when instructed to do so by an instructor when required in a course. The IT Department is responsible for installing and removing all other software applications. Users may not load personally owned software on Heartland Community College devices.

3.3.2 Internet Downloads

Users may not willfully download any applications from the Internet which may be destructive or interrupt network services to other students and users onto Heartland Community College owned computers.

3.3.3 Software and Internet Use

Information available through the computer and network systems, including the Internet, may be distracting, objectionable, or even disturbing. Since computers may be visible or audible to others, sensitivity in viewing and/or listening to such material is requested. Computer users who disturb or distract others may be asked to stop their activities or leave the area. Some courses utilize software applications which may be disruptive to others using the open lab. Consequently, these applications are accessible to students only in special purpose labs.

3.3.4 Pornography

Users may not use any Heartland Community College owned technology resource for purposefully accessing images, sounds, or messages that are pornographic in purpose. *This does not apply to legal, sexually explicit literary/artistic expressions or materials that are relevant and appropriately related to course subject matter or curriculum.*

3.4 Hardware

3.4.1 Physical Misuse of Resources

General physical misuse including theft, any unauthorized loan or removal of equipment from campus, damage or destruction is prohibited.

3.4.2 Installation/Removal of Hardware

The IT Department is responsible for acquiring, installing, moving, and removing all college hardware devices in all areas including but not limited to classrooms, computer labs, and office areas. Users may not move, change, or install hardware.

3.4.3 Use of Standard Media Devices and Peripherals

Users may use personally owned media and memory devices including diskettes, USB drives, CD-ROMs, headphones, etc. in any college owned equipment. However, the college cannot be responsible for any damage to or loss of information from these devices due to viruses, hardware malfunctions, or any other threats.

3.5 System Integrity

The Policy may be viewed at: www.heartland.edu/policy/appropriateUseAtHeartland.pdf

Users shall not:

3.5.1 Intentionally infiltrate or “hack” HCC computing systems.

3.5.2 Willfully create and/or release viruses, worms, or other programs that damage HCC’s network or an outside network.

3.5.3 Conduct large-scale distribution of such things as MP3 music or video files.

3.5.4 Knowingly or recklessly download or distribute excessively large files, large numbers of digital audio or video files, or audio or video streams.

4.0 USERS’ ROLE IN SECURITY

Each person granted access to specific college secured resources must comply with the following college data security and confidentiality requirements, and applicable laws.

4.1 Login Name and Password Policy

Users will construct secure, private passwords. Users are responsible for protecting their passwords from discovery by others and must immediately change any compromised password.

4.1.1 Sharing of Login Names and Password

A user may **NOT** transfer or share any Login Name or password with any other person. Use of another user’s Login Name or password is prohibited.

Violation of the security policy will be documented and reported to the Information Security Officer.

4.1.2 Security Compromise

The Systems Administrator has the authority to disable any user’s account if there is evidence of hacking attempts or reason to believe a password has been compromised.

4.1.3 Failed Password Attempts

Accounts have security protocols that will automatically disable the account after a specific number of failed login attempts. When an account becomes disabled, the user must contact the IT Department to have the account reactivated.

5.0 PRIVACY & RESOURCE ACTIVITY MONITORING

Heartland Community College respects the privacy of the individual. It is not the practice of College administrators or employees of the Information Technology department to access the files created and stored by others or routinely monitor the use of technology resources. Although privacy is valued, it must be balanced with the requirements of assuring system integrity. Consequently, it may be necessary for the Systems Administrator to monitor activity and/or access to files without the consent of the user. The scenarios by which this may occur include, but are not limited to the items listed below.

5.1 Maintenance

Systems Administrators regularly scan volumes of data on network devices for routine maintenance purposes and may see the contents of files.

The Systems Administrator is required to report any illegal activity that is discovered, or any information that indicates a violation of policy to the Information Security Officer, who will review the report with a Cabinet member. Policy violations will be pursued in accordance with Section 7.0.

The Policy may be viewed at: www.heartland.edu/policy/appropriateUseAtHeartland.pdf

5.2 Access Without Consent

When file access without consent is deemed necessary, the Information Security Officer, the Chief Information Officer, or a member of the Cabinet will authorize access. The Systems Administrator or designee will log all instances of access without consent. Situations that may result in file access without consent include, but are not limited to the following:

5.2.1 Emergency Entry

Emergency entry may be necessary to preserve the system infrastructure and integrity, and facilities or to preserve public safety.

5.2.2 Reasonable Cause

Heartland Community College reserves the right to examine files should reasonable cause exist to believe an individual has violated internal policy, state or federal law. When an user other than a Systems Administrator is more qualified to research a specific violation, the Information Security Officer or the Chief Information Officer, in consultation with a Cabinet member, may authorize granting temporary access to another Heartland Community College administrator so that he or she may research the alleged violation.

6.0 INFORMATION PRIVACY PRACTICES DISCLOSURE

Users who conduct financial business with the college may obtain a copy of the Heartland Community College Information Privacy Practices document on the College website. Changes to the policy will be reflected on the website within 30 days after the change.

7.0 VIOLATION AND ENFORCEMENT PROCEDURES

Heartland Community College considers any violation of appropriate use guidelines to be a serious offense. Violators of this policy may be subject to disciplinary action in accordance with this policy and the student conduct policy, up to and including dismissal from the college and/or termination of access to computing resources. In addition to college discipline, violators of this policy may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT resource.

8.0 POLICY MAINTENANCE AND DEVELOPMENT

This policy document, as well as all appendices, addendums, procedures, and reference materials are available to all users through the College website.

This policy will be reviewed annually, or as needed, as is determined by the Information Security Officer. Concerns or questions about the policy may be directed to the Information Security Officer, the Chief Information Officer or the Vice President of Business Services.