Acceptable Use of Computing and Information Technology Resources

Version 1.6, December 18, 2015

General Statement

As part of its educational mission, Hocking College acquires, develops, and maintains computers, computer systems, and networks. These computing resources are intended for college-related purposes, including direct or indirect support of the College's instruction, service and research missions; college administrative functions; student and campus life activities; and the free exchange of ideas within the college community and among the wider local, national and global communities.

The rights of free expression and academic freedom apply to the use of college computing resources and network. So too, however do the responsibilities and limits associated with those rights. All who use the College's computing resources must act responsibly, in accordance with the highest standard of ethical and legal behavior. Thus, legitimate use of computer resources or network does not extend to whatever is technically possible and all users must abide by applicable restrictions.

The computer network and all associated equipment are the property of Hocking College and are to be used for academic and business purposes. Hocking College strives to provide the most efficient, cost-effective technology and systems to assist students and employees to succeed academically and perform their jobs. Students and Employees, however, do not have an expectation of privacy in the Hocking College owned and provided systems and equipment.

Applicability

This policy applies to all users of college computing resources and network, whether affiliated with the college or not, and to all uses of those resources, whether on campus or from remote locations.

The policy outlines the standards for acceptable use of college computer resources and network that include but are not limited to equipment, software, networks, data, and telecommunications whether owned, leased or otherwise provided by Hocking College.

The use of any Social Media including, but not limited to Facebook, Twitter, LinkedIn, Instagram, blogs, Flickr and YouTube shall not be used to discriminate, harass or retaliate others, and an allegation that social media has been used in such a manner will be treated by Hocking College like any other allegations of such behavior, including conducting an investigation and taking disciplinary action where appropriate.

Additional policies may govern specific computers, computer systems or networks provided by or operated within specific departments of the college.

Policy

All computing resource and network users must:

1. **Comply with all federal, Ohio, and other applicable law; college rules and policies; and the terms of applicable contracts and licenses**. Examples of such laws, rules, policies, contracts and licenses include but are not limited to:
    a. Laws of libel, privacy, copyright, trademark, obscenity, and child pornography.
    b. The Electronic Communications Privacy Act
    c. Computer Fraud and Abuse Act, which prohibit “hacking”, “cracking”, and similar activities.
    d. Family Educational Rights and Privacy Act (FERPA)

    In particular, FERPA:
        i. FERPA permits College employees to have access to student education records in which they have "legitimate educational interest." Such access does not require prior written consent of the student.
        Essentially, legitimate educational interest is necessary for employees to carry out their responsibilities in support of Hocking College’s educational mission. You can also think of legitimate educational interest as a "need to know" that is essential to carrying out your job responsibilities related to education.

        It is important to understand several points related to "legitimate educational interest:"

            1. Curiosity is not a legitimate educational interest. Just because you have access to the College’s information and are able to

view the record of your neighbor's son, does not mean that you have a legitimate educational interest in his grades and cumulative GPA.

2. Simply the fact that you are a College employee does not constitute legitimate educational interest. Your need to know must be related to your job responsibilities in support of the College's educational mission. In other words, records should be used only in the context of official business in conjunction with the educational success of the student.
3. Your legitimate educational interest is limited. While you may have a need to access education records for students, you do not necessarily have a similar need to view records of students outside your college. In other words, access to information does not authorize unrestricted use.

e. Health Insurance Portability and Accountability Act(HIPAA)
f. Hocking College code of student conduct
g. Hocking College Administrators' Manual, Faculty Handbook
h. Hocking College sexual harassment policy
i. All applicable software licenses and contracts

In particular, users must:

j. Respect copyrights, intellectual-property rights, ownership of files and passwords. Unauthorized accessing or modifying (including altering information, introducing viruses or Trojan horses, or damaging files) is unethical and may be illegal. Additionally, unauthorized copying of files or passwords belonging to others or to the College may constitute plagiarism or theft.

Hocking College extends these licenses , contracts, policies and guidelines to systems outside the college that are accessed via the college's computer resources and network (e.g.; electronic mail or remote access activities utilizing the college's network).

Further, users who engage in electronic communications or activities with persons in other states or countries or on other systems and networks should be aware that they may also be subject to the laws of those states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

2. **Use only those computer resources that they have been authorized to use and only in the manner and to the extent authorized**.

   Accounts and passwords may not, under any circumstances, be used by persons other than those to whom they have been assigned. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change their password and report the incident to the Information Technology Helpdesk.

   Ability to access or share computing resources or College information does not, by itself, imply authorization to do so. Access to the College's computer resources and network is a privilege and use should be limited to only their intended purposes.

3. **Respect the finite capacity of resources and the network and limit so as not to consume an unreasonable amount of resources or to interfere unreasonably with the activity of others**. Although there is no set bandwidth, disk space, or other limit applicable to all uses of college computer resources, the college may require users of those resources to limit or refrain from specific uses in accordance with this principle. The college reserves the rights to limit, restrict, or extend access to information technology resources.

4. **Refrain from using computing resources or network for commercial purposes.** Personal non-commercial use of college computing resources is permitted when it does not consume a significant amount of these resources, is in compliance with this and other college policy, and does not interfere with the college's responsibilities.

5. **Refrain from stating or implying that they speak on behalf of the College.** Users must also refrain from use of College trademarks or logos without authorization to do so. The use of suitable disclaimers is encouraged.

6. **Refrain from issuing true threats or fighting words.** Obscenity; defamation; violations of criminal law; violations of the student code of conduct; materially disruptive speech, harassing speech, Title IX and violations of program standards are not protected, and will not be considered protected speech under the First Amendment

   Authorization for use of College trademarks and logos must be approved. Guidelines

for college faculty are available within the Style Guide posted on the College's faculty intranet site.

Enforcement

Whenever it may become necessary to enforce college policies or when alleged violations occur, the college may temporarily suspend or block access to a computer resource or to the network, prior to the initiation or completion of sanctions, when it reasonably appears necessary to do so in order to protect the integrity, security and availability of college resources and information or protect the college from liability. Additionally, the College may undertake audits of systems, information or resources where policy violations are possible.

Sanctions

Violations of this policy may result in denied access to college computing resources and users may be subject to other penalties and disciplinary action, both within and outside the college.

Violations will normally be handled through college disciplinary procedures applicable and described in the Student Code of Conduct, Employee Handbook, Support Staff Agreement, and Professional Unit Agreement. Employee violations will be referred to Human Resources; Student violations will be referred to Campus Judiciaries for appropriate handling.
The college may refer suspected violations of applicable law to appropriate law enforcement agencies.

Security and Privacy

This Acceptable Use of Computing and Information Resources Policy gives Hocking College the clear right to monitor, investigate and take appropriate action to remedy any misuse or abuse of these resources. The college employs various measures to protect the security and confidentiality of its computing resources and of their users' accounts. Users should be aware, however, that the college cannot guarantee such security or confidentiality. Users should therefore engage in "safe computing" practices by guarding their passwords and changing them regularly.

Users should also be aware that their uses of College computing resources are not private. While the college does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of college computing

resources require the caching and backup of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the delivery of service. Additionally, systems or information technology administrators, as part of their technical responsibilities may occasionally need to diagnose or solve problems by examining the contents of particular files.

The college may also specifically monitor the activity and accounts of individual users of college computing resources, including login sessions, content of communications, without notice when:

a. The user has voluntarily made them accessible to the public.
b. It reasonably appears necessary to do so to protect the integrity, security or availability of college or other computing resources or to protect the college from liability.
c. There is reasonable cause to believe that the user violated or is violating this policy.
d. An account appears to be engaged in unusual or unusually excessive activity as indicated by the monitoring of general activity and usage patterns.
e. It is otherwise required or permitted by law.

The college, at its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of communications, to appropriate college personnel or law enforcement agencies and may use those results in appropriate college disciplinary proceedings.

Communications made by means of college computing resources are also subject to the Ohio Public Records Law to the extent as they would be if made on paper.

Additional Contacts

Submit comments, questions, and suggestions to the Hocking College IT Helpdesk at helpdesk@hocking.edu or 753-6113.

Review of Policy

This policy may be reviewed and updated from time to time to reflect substantial changes to the information technology resources or changes in legal statutes that impact computing resources, copyright, intellectual property or privacy. The Hocking College CIO is responsible for determining when the policy needs to be assessed and revised.

Other Hocking College Computing Policies

- IT Guidelines: Mailing Broadcast or Bulk Email Messages

Frequently Asked Questions (FAQ)

What if I'm using my personally purchased computer? Does this policy still apply?

Yes, the policy applies when you are connected to the Hocking network (wired or wireless) and using the connectivity it provides.

What is considered a legitimate situation for account sharing?

The practice of individual user account sharing is prohibited. The only time this activity should occur is with direct coordination with the Office of Information Technology.

If you believe your account can be or has been accessed by someone else, you should change your password immediately.

What is a secure password?

An ideal password is long and has letters, punctuation, symbols, and numbers.

- Whenever possible, use at least 8 characters or more.
- The greater the variety of characters in your password, the better.
- Use the entire keyboard, not just the letters and characters you use or see most often.

Avoid creating passwords using:

- Dictionary words in any language.
- Words spelled backwards, common misspellings, and abbreviations.
- Sequences or repeated characters. (Examples: 12345, 222, abcde, qwerty).
- Personal information. (Examples: name, birthday, driver's license number).

When the policy states that the college may monitor the activity of accounts, does that mean my instructor or department chair can access my files and email?

No. The only staff authorized and with the privileges required to conduct direct monitoring are within the Office of Information Technology.

Monitoring means that network usage is noted, unusual connections (indicative of malicious outside users hijacking the current systems) may be investigated, and under those circumstances, email and some files may also be reviewed by Hocking IT personnel. .

I have observed a violation of this Acceptable Use Policy. What do I do?
Violations of this policy should be reported to the IT Helpdesk at helpdesk@hocking.edu or 753-6113.

Definitions

Computer Resources - Includes but are not limited to computing equipment, software, networks, data, and telecommunications whether owned, leased or otherwise provided by Hocking College.

Safe Computing -The practice of choosing a secure password, keeping software up-to-date, installing anti-virus software and backing up data.