312 TECHNOLOGY USE POLICY

Technology resources are valuable, and their abuse can have a far-reaching negative impact on the entire campus. The same standards that apply in the non-computing environment apply in the computing environment. In providing computing resources, WCCC has the responsibility to inform its users (faculty, staff and students) of the rules and procedures regarding their usage. Users are responsible for understanding these rules so that they can abide by them.

Policies regarding conduct generally address issues such as treatment of other individuals, theft, destruction of property or vandalism, and access (i.e. who can use what and when). The WCCC Technology Use Policy is intended to address these elements as they relate to the evolving landscape of computing, network, and information resources. Because technology changes so quickly, no policy dealing with it can hope to remain current in all its details. The policies delineated here should be considered examples, and not an exhaustive list of prohibited behavior. Unauthorized use has two meanings regarding technology issues. First, it can mean that an individual is not authorized to use a machine, network, or other resource, for any purpose. Second, it can mean that although an individual is authorized to use a particular resource, certain activities are prohibited.

As with all other organizations, standard, responsible systems administration requires close monitoring by WCCC network administrators of the usage of College information systems. E-mail is not guaranteed to be private or confidential. All electronic communications are College property. When necessary to investigate violations of these and other College policies, the College will examine the contents of "personal" directories, e-mail folders, and other resources accessible to users. Such examinations are not done frivolously. They are conducted only by the Office of Information Technology, under the direction of the Vice President of Finance and Operations, unless directly ordered otherwise by the College President.

I. Introduction

It is essential for all users to practice ethical behavior in their use of technology resources since they have access to many valuable resources and their computing practices can adversely affect the work of other users. Most users act responsibly, but the few who do not, either through ignorance or by intent, have the potential for disrupting all users' work. Warren County Community College (WCCC) has the responsibility of securing all technology systems to a reasonable and economically feasible degree against unauthorized access while making systems accessible for legitimate and innovative uses. This responsibility includes informing users of an expected standard of conduct and the punitive measures for not adhering to them.

The following list constitutes a code of technology practice for users. Disciplinary action for violating the code shall be governed by the applicable provisions. Violations may also result in criminal prosecution under State and/or Federal law. Every student, employee, instructor or other person using the College's information technology systems agrees to abide by the tenets set forth in the following policy.

II. Access

A. Users may only use network accounts that have been authorized for their use.

B. Users must identify work produced through technology with their own names so that responsibility for the work can be determined and users can be contacted in unusual situations, e.g., the return of misplaced output.

C. Users must use their network accounts solely for the purposes for which they were authorized.

D. Users must not attempt to modify WCCC technology equipment or resources.

E. Users must not attempt to subvert the restrictions associated with their computer accounts.

F. The College has password protocols established to ensure that each user has a unique password when an account is set up as well as a self-service password system to assist students. Users are responsible for the usage of their computer accounts. Users are required to maintain secure passwords for systems that support them and take precautions against others obtaining access to their computer resources. Each user is responsible for all transactions made under the authorization of his or her system account.

III. Use

WCCC's technology resources, including hardware, software, wired and wireless networks, are provided for the use of students, staff and faculty in fulfilling their needs that relate to the mission of the College. Other usage is prohibited. This includes, but is not limited to:

A. Unauthorized access of a file to use, read or change the contents, or for any purpose.

B. Unauthorized transfer of a file.

C. Unauthorized use of another individual's network account. .

D. Use of WCCC technology resources to interfere with the work of another student, faculty member or College official.

E. Use of WCCC technology resources to send or receive what may be deemed under the circumstances to be obscene or inappropriate.

F. Interference with normal operation of the College's network systems or databases.

G. The utilization of a network access account for the purposes of development and/or utilization of malicious code or viruses, The only exception would be if materials were developed as part of a class assignment under the explicit direction of a faculty member. This activity must be authorized in advance by the Office of Information Technology.

H. Solicitation for charity, personal needs or other organizations/persons without approval of the College.

I. Activities related to the promotion and/or running of a personal for-profit venture or other activities unrelated to the provision of an undergraduate education.

J. Using WCCC technology to undertake harassment or behavior that is in violation of the Campus Code of Conduct..

K. Promoting and sending chain letters, mass mailings or personal advertisements using college technology resources.

L. Sending electronic communications or email that obscures the identity of the sender, misrepresents the College or represents the sender as someone else.

M. Harassing students or employees at the College or other organizations.

N. Sexual, racial, ethnic, religious or any other harassment of any individual or group of individuals.

O. Access to websites, listservs, software and other resources that do not provide a scholarly treatment of pornography, hate speech, or activity, which otherwise would be deemed a violation of existing law. When the scholarly merit of such materials is in question, the judgment of the College administration will be final.

P. Misuse, intentional damage or loss of technology equipment owned by WCCC.

Q. Use of technology equipment without appropriate safeguards to protect sensitive college documents.

R. Use of technology systems in a way that violates Copyright policies or laws (see Policy 404 for additional information).

S. Any other uses prohibited by WCCC policies and/or state or federal regulations or statutes.

All electronic communications through the College's network are considered College property. Employees must be aware that certain communications may be considered public and therefore subject to the State's Open Public Records Act. As a result, the College reserves the right to examine, monitor and regulate communications and network usage of employee and student accounts.

The College also reserves the right to manage the technology network, equipment and infrastructure to ensure that the educational mission of the WCCC can be served. This may mean include the blocking or limiting access and usage of network service to individually paid subscription services or gaming sites.

Nothing above or herein is intended to violate "Academic Freedom." Under "Academic Freedom," material otherwise not appropriate for use on the College's technology or networks will be exempt from this policy. However, the College shall not protect or indemnify employees who access materials that are considered illegal and monitored by law enforcement officials (example: child pornography sites). To avoid any misunderstanding, it is required that any instructor consult with the Academic Vice President prior to the use of questionable, controversial or potentially offensive print or digital materials.

IV. Individual Rights, Privileges and Responsibilities

A. Members of the WCCC community have the right to be free of harassment. Usage of the College's technology systems to violate this basic right is strictly prohibited and will be treated with the utmost gravity.

B. The College understands that providing network connectivity and advanced technology often facilitates personal and recreational usage of those systems. However, the use of the College's technology systems for activities not directly related to learning (for students) or performing of work duties (for staff and faculty) is a privilege. While these activities are not encouraged, they are tolerated so long as they:

1) do not infringe on the rights of other users to use the College systems for bona fide academic or work-related activities
2) do not interfere with the accomplishment of one's work responsibilities
3) do not violate any other portion of these technology use policies.

C. The use of the College's wireless infrastructure for the purposes of streaming third- party, non-academic content is strongly discouraged. The College reserves the right to restrict non-academic content to ensure adequate bandwidth for instructional needs. The college offers no guarantee of access to third- party, non- academic content through personal devices. Wireless access privileges may be revoked at any time for failure to comply with any of the above listed requirements.

D. As a function of accepted and responsible system management, network administrators may conduct examinations of any or all files on the network to monitor compliance with these usage policies and to insure the effective and appropriate functioning of WCCC technology infrastructure. This is a legal right of the College and any other organization that provides similar systems for the execution of its mission.

E. The College regards electronic and voice communications as vehicles for the delivery of information and not as mechanisms for the retention or archiving of such information. It is the responsibility of the individual sender and/or receiver of such messages to determine which information should be retained or archived. Records retained by an individual, even if they are retained on an electronic medium, are subject to College policies, State and Federal laws.

V. Software

A. Warren County Community College licenses the use most of its computer software applications from external vendors. The College does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce or modify it.

B. Users agree not to copy, disclose, transfer, or modify, without written permission, any computer software or documentation that the College provides its users. The sole exception to this policy is software clearly marked as belonging to the public domain.

C. Media containing licensed software and the accompanying documentation is to be used in College office areas, classrooms, and computing labs, and is not to be removed from such designated areas.

D. All use of software provided by WCCC and all use of the College's computer and telecommunications equipment is subject to vendor license agreements, this policy statement, and applicable Federal and State law. Users agree to comply with all such restrictions.

VI. Secure Device Policy

Warren County Community College issues various types of technology equipment to employees in order to ensure that college services can be effectively provided to students and the Warren County community. This equipment may include workstations, laptop, notebook and tablet computers or other technology devices. Employees issued these devices are permitted to use

the equipment off campus solely for work-related activities unless otherwise authorized by the Board of Trustees Employees must return all equipment upon separation from the College.

College devices intended for students are not intended to leave the campus. However, in an emergency circumstance (such as the COVID-19 pandemic) equipment may be loaned temporarily to students. All users of college-owned devices are expected to return devices to the College at the end of a loaner period or the end of an assignment or semester.

In order to best secure student and employee data, all college-owned computing equipment containing confidential or intending to store college data that leaves the College campus shall be protected with encryption technology. The College shall maintain procedures for the securing equipment in accordance with the accepted industry encryption standards.

VII. Enforcement

A. Complaints against any user for violation of these policies shall be the subject of full and immediate investigation and may result in the suspension or revocation of access to WCCC technology or other sanctions in accordance with College policy.

B. Users wishing to make a complaint or report violations of these policies should contact the Vice President of Finance and Operations.

C. Revocation of access may be done at any time by the Office of Information Technology to protect users' rights and privileges and to safeguard College resources.

D. If violations of these Technology Use Policies occur, those responsible for such abuse will be held accountable and may be subject to disciplinary action and may also be subject to criminal investigation, as warranted.

E. Violations to these policies will be forwarded to the Vice President of Finance and Operations at (908) 835-2355 for disposition and action. The Vice President may, at his or her discretion, involve other individuals to assist in resolution of the matter. When deemed necessary, the College may consult or turn the matter over to the appropriate legal authority.

F. Any employee who abuses the privilege of the College-facilitated access to email, the internet or the use of hardware or software may be subject to disciplinary action up to and including termination of employment.

Approved: 12/17/14
Revised: 2/14/18
Revised: 9/16/20