WARREN COUNTY COMMUNITY COLLEGE
TECHNOLOGY, DATA AND INFORMATION POLICIES

Table of Contents

About this document

This document is a compendium of the Board of Trustees information technology and computer-related policies. It is not intended to be an exhaustive list of all college procedures related to IT. Please consult the IT office (support@warren.edu) if you have specific IT questions or needs.

312 Warren County Community College's 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 needsor 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: 02/14/18
Revised: 09/16/20

203 Social Media Policy

This policy governs employees of the Warren County Community College who utilize a variety of social media technologies. It is not limited to any specific media format.

Social Media Defined:

For the purpose of this policy, social media is defined as any internet or mobile digital technology and systems used to share and/or receive information or conversation. This policy is intended to cover public social media (as opposed to College media such as a Learning Management System). Use of College media is covered under the Technology Use Policy (Policy 312).

Social Media Personal Site Guidelines:

WCCC respects the individual rights of its employees to participate in social networking activities. The College also recognizes its responsibility to communicate to employees the professional risks associated with participation in a non-work related social networking. If an employee enters into an interaction on social media, the employee risks being exposed to public reaction that may call into question his/her integrity and professionalism. Therefore, it is the position of WCCC to encourage faculty and staff to exercise caution when participating in social networking.

Below are some key guidelines to assist employees:

1. Employees should remember that the public may judge WCCC based on the utterances of an individual employee. Hence, employees, when participating in a social networking site, should attempt at all times to be accurate, exercise appropriate restraint, show respect for the opinion of others, and not subject the institution to public embarrassment or negative attention.

2. WCCC's mission is to serve the Warren County region. An employee who strongly disparages the students, employees or citizens served by the College can impair WCCC's ability to carry out its mission. Employees must recognize that members of the public may not necessarily distinguish between an employee's public vs. personal persona on social media. Therefore, individuals must act judiciously when posting information or materials about the College or the local community.

3. Employees should be aware that they may be held legally liable for what is posted on their own site and on the sites of others where they have attributed information. Conversely, the College cannot be held liable for the utterances of an employee acting without the expressed written approval of the College.

4. Unless posting on social media during paid working hours is part of an employee's employment assignment, an employee shall not undertake social media activity during paid work time.

5. WCCC email addresses are intended solely for College business. Employees shall not use their WCCC email address for any non-WCCC related commercial or social media activities unless it has been pre-approved by the College.

6. Employees may not use social media to publish confidential materials of the College.

7. Employees should use only official college communication networks to conduct college business. The use of the College name, logo or image to advertise events or to solicit business on social networks is prohibited without prior College permission.

8. Employees are free to endorse whatever product, cause or political party that they desire, as long as such endorsement does not have the appearance that it is related to the employee's employment or affiliation with Warren County Community College. The use of the College name to promote or endorse any product, cause or political party or candidate is prohibited.

9. The lines of professional and personal relationships can become blurred in a social media situation. Communication on social media with other employees and, especially, individual students, has the potential to create confusion regarding the role of the employee who is posting or commenting on information. Employees are cautioned to ensure that they maintain a professional relationship on social media with students and colleagues. In particular, employees should be careful not to open themselves up to possible complaints of a violation of college harassment, bullying or intimidation policies based on an employee-student or employee-employee relationship.

10. Employees are advised to take care to ensure that their social media activities reach the audience that is intended. The use of privacy settings can significantly reduce the possibility that a casual remark, joke, etc. is not misinterpreted by someone who was not intended to see the information.

11. Employees should be mindful that the posting of items anonymously does not necessarily guarantee future anonymity. An employee who posts patently malicious, false, misleading or hateful comments may be held professionally liable for such speech should his/her identity subsequently be determined.

WCCC respects the rights of its employees to act as private citizens. However, it cannot ignore legitimate employee, student or public complaints made about employee behavior off-campus and through social media. An employee should not assume that academic freedom or private speech rights inherent in higher education provide a "safe harbor" from any sanctions for egregious violations of this social media policy.

The College is required to follow up on any reports or information regarding suspected criminal behavior by one of its employees. Any employee conduct on social media that appears to be in violation of federal, state or local statutes is subject to investigation by either the College and/or law enforcement agencies. If any violation of policy or law is discovered, the employee will be disciplined accordingly.

Approved: 06/24/15
Revised: 06/26/19

304.3 WCCC Standards of Community Conduct

The following standards and regulations are designed to protect the rights, privileges and property of all individuals associated with the College. Misconduct in any of these categories is subject to disciplinary action.

A. Any and all laws of the State of New Jersey, County of Warren, Township of Washington, and Town of Phillipsburg that provide for the protection of persons; for the protection of personal, real or public property, or provide for the regulation of motor vehicles, shall apply and be in effect on College property and such laws shall be properly enforced.
B. Students who violate the law may incur penalties prescribed by civil authorities, but College authority is never used merely to duplicate the function of general laws. Only where the interest of the College as an academic community is distinctly and clearly involved will the authority of the College be asserted.
C. The campus locations in Washington and Phillipsburg shall regularly be open and available for use by the public daily, including any designated hours during the weekend.
    1. No one will be permitted into any classroom, office, library, building or campus grounds at either location before opening time or after closing time without proper authorization.
    2. No unauthorized vehicles will be permitted on the campus of either location after closing.
    3. The schedule and regulation shall be in effect unless special conditions shall exist. Notice of the special conditions and scheduled changes shall be given by the President or his designated agent.
D. Use, possession, manufacture, distribution or sale of illegal or controlled substances (as defined by federal, state and local statutes) on College property or at college sponsored events is prohibited.
E. Possession, use or distribution of alcoholic and intoxicating beverages on College property is prohibited. Use of such beverages outside of the law at College events on and off campus is prohibited. See the *College Substance Abuse Policy* for greater specificity.
F. Gambling on College property as defined in the State Criminal Code shall be prohibited and enforced in accordance with state law.
G. Use, possession or concealment of any firearms, fireworks, explosives, dangerous chemicals or any other material or weapon considered deadly or dangerous on College property is prohibited.
H. Endangering or infringing upon the personal safety, personal rights or personal property of any member of the campus community is prohibited.
I. Threatening, intimidating, coercing or using physical force in a manner which causes another member of the campus community to be injured or fearful of physical harm is prohibited, including assault, battery and sexual offenses.
J. Any form of intimidation or harassment toward any member of the College community is prohibited.
K. Slandering or libeling another member of the College community is prohibited.
L. Displaying indecent or obscene conduct (in violation of federal, state and local statutes) to another member of the College community is prohibited.
M. Willful defacement, destruction or misuse of public and private properties is prohibited.
N. Theft, larceny or embezzlement of public and private property, including issuance of bad checks is prohibited.

O. Interfering with regular College operations including, but not limited to, teaching and classroom activities, administration, meetings and public discussions, disciplinary procedures, College activities, and fire, police or emergency services is prohibited.
P. Dishonesty such as cheating, plagiarism or otherwise intentionally furnishing false information to the College is prohibited.
Q. Unauthorized use of computers, or computer services and time is prohibited.
R. Forging, altering or misusing any college document or instrument of identification is prohibited.
S. Using the College name for soliciting funds or other activities without prior permission is prohibited.
T. Operating a vehicle in a reckless fashion on College property is prohibited. All traffic or vehicle regulations shall be strictly enforced by the College.
U. Violating the College standards of conduct while participating as a student at off-campus sites or at events where the student is representing the College or engaging in any behavior or practice that is determined by college faculty, staff or auxiliary staff to be injurious or hazardous to other persons is subject to involuntary withdrawal from the program and disciplinary action.
V. Failure to comply with direction of College officials when those officials are acting in performance of their duties and are requesting the student behave in accordance with college policies and regulations.
W. Any type of cyber-harassment, including electronic stalking, bullying, and/or sexual exploitation.
X. Student organizations are collectively responsible for any action committed by members on behalf of their organization that violate College policy. Disciplinary action against student organizations is separate from actions taken against individuals. Facts of an incident may necessitate action against both a student organization and the individual members of that organization who were found to have violated College policy.
Y. Obstructing the free flow of pedestrian or vehicular traffic on or adjacent to College premises or at College events is prohibited.
Z. Students are required to comply with the reasonable and lawful directions of College officials and College security.
AA. Making, attempting to make, or transmitting an audio or video recording of private, nonpublic conversations and/or meetings on College premises without the knowledge and consent of all participants subject to such recordings. This provision does not extend to the recording of public events or discussions, or to recordings made for law enforcement purposes.
BB. Violating other published College regulations or policies.

Approved: 03/23/05
Revised: 11/19/08
Revised: 03/23/16
Revised: 12/16/20

306 Privacy Rights of Students

The purpose of the Family Educational Rights and Privacy Act (FERPA) is to protect the privacy of students and parents, and to notify students and their parents of their rights to privacy as provide under Section 438 of the General Education Provisions Act as amended. Warren County Community College will comply with all aspects of the FERPA law and regulations.

It is the policy of Warren County Community College to allow students access to certain records maintained by the College and to provide an opportunity to challenge the accuracy or appropriateness of such records.

306.1 PROVISIONS

I. Students enrolled at Warren County Community College have the right to inspect and review their educational record. If any material or document in the educational record of a student includes information on more than one student, each student will have the right to inspect only that part of the material or document that relates to him or her.

II. College students are considered adults under F.E.R.P.A. and therefore determine who will receive information about them. Student academic information such as grades or academic standing (GPA, academic transcript, etc.) will be given to the student, regardless of age or financial situation. Students may opt to release information in writing to parents or other individuals as specified.

III. The Vice President of Student Services of WCCC has the responsibility for maintenance of the educational record and other documents relative to the student's enrollment and academic progress.

IV. Warren County Community College will comply with all aspects of the General Data Protection Regulation legislation as it pertains to community colleges in the United States.

306.2 EDUCATIONAL RECORD

The term educational record includes only the following materials and documents:

A. Applications for admission and re-admission
B. High School transcripts or GED score reports
C. College transcripts
D. Registration and Drop/Add forms
E. Placement test results and waiver forms
F. College communications pertaining to academic matters
G. Transcripts of academic grades and semester grade reports
H. Letters of reference prepared by Warren County Community College
I. Final grades
J. Transcript evaluation for transfer credit
K. Instructor referral forms
L. Admissions decision sheets
M. Copies of letters written by WCCC to a third-party confirming enrollment status
N. Correspondence between the College and the student, which directly pertains to matters of requisition, academic progress, grades or any other item of the educational record
O. SAT/ACT and/or Accuplacer or other standardized test score reports

The above list is intended to describe what may be found in educational records. Not all documents pertain to all students, nor are all the documents described above required for all students. Many of the documents listed above may be stored in electronic format in lieu of paper copy.

The term educational record does not include the following:

A. Financial records of parents or students
B. Confidential letters and statements placed in the student's file
C. Counseling or advising notes
D. Records of administrative and teaching faculty which are in the sole possession of the faculty and which are not accessible to or revealed to any other person except a substitute instructor
E. Confidential recommendations regarding admissions, honors and awards, or employment if the person has signed a waiver of his/her right to access this information. Such a waiver shall apply to recommendations only if:
    1. The statement is, upon request, notified of the names of all persons making confidential recommendations
    2. Such recommendations are only used for the purpose intended
F. Medical records
G. Disability records
H. Disciplinary records

306.3 DIRECTORY INFORMATION

Warren County Community College may release the following ""directory"" information on any student unless the student has designated that it should not be released without his/her prior consent. Such notification must be submitted by the student in writing to the Office of Student Services.

A. Student Name
B. Participation in recognized school activities
C. Dates of attendance
D. Degrees, Certificates, and awards received from WCCC

Nothing hereinabove shall limit the College from modifying the list of “directory information” in accordance with changes in federal or state guidelines.

Warren County Community College will not release the educational records or personally identifiable information of its students (other than directory information) without the written consent of the student to any party, except as permitted under federal law.

Students requesting that their directory information not be released must follow the procedures established by the Office of Student Services and contained in the Student Handbook.

306.4 STUDENT ACCESS TO THEIR OWN RECORDS

Students may access their own records in accordance with procedures established by the Office of Student Services and published in the Student Handbook. In addition, students may obtain copies of any material or document contained in their educational record, except official copies of documents received from other institutions or agencies, such as high school or college transcripts. The cost for copies of educational records is as follows:

1 to 10 pages .... @ $0.75 per
11 to 20 pages .... @ $0.50 per
20+ pages .... @ $0.25 per

Students will be required to pay the cost of special mail handling (e.g., overnight or registered mail)

Students may request explanations and interpretations of any portion(s) of their educational record through the procedures outlined in the student handbook. The College shall offer students an opportunity to make any corrections to their records and an opportunity for a hearing to challenge items in their student file.

Approved: 12/15/04
Revised: 06/30/10
Revised: 04/18/18
Revised: 4/15/20

506.1 Security of Financial Information

Warren County Community College is subject to various federal requirements to secure the financial information of students. Policy 501.6 enumerates the actions that the College will continue to undertake to secure financial information.

501.6.1 GRAMM-LEACH-BLILEY ACT

Under the 2000 Gramm-Leach-Bliley Act (G-L-B Act), the College is considered a financial institution because two of the College's activities ("making, acquiring, brokering, or servicing loans" and "collection agency services") are consistent with banking industry functions under the Bank Holding Company Act of 1956. As a result, the College must comply with two requirements of the G-L-B Act: Privacy of Consumer Information (Privacy Rule) and Safeguarding of Consumer Information (Safeguards Rule).

A) Privacy of Consumer Information

The privacy of student information contained in the G-L-B Act is consistent with the privacy responsibilities that colleges and universities must follow under Family Educational Rights and Privacy Act (FERPA). As such, Warren Community College will continue to ensure the privacy of student records, including their financial records, under Policy 306: Privacy Rights of Students, to satisfy the Privacy Requirements of the G-L-B Act. In addition, where applicable, the College shall comply with the safeguards of information for students covered under the General Data Protection Regulation (the European "Right to be Forgotten" law).

B) Safeguarding of Consumer Information

WCCC is committed to safeguarding the financial information of students and members of the campus community. As such, it has developed the following standards to safeguard financial information for students and employees (hereafter "customers"):

1) Electronic Safeguards

a. Electronic customer information is stored on secured servers. All servers are password protected and unauthorized access is protected via a series of firewalls and other protections. Network security is routinely tested and subject to security audits.
b. Servers are routinely backed-up and the back-up information is stored off-site.
c. Employees are advised to maintain all work product on network drives to ensure that materials are backed up daily.
d. Anti-virus software is routinely used. Security patches are installed as necessary, according to the latest industry standards.
e. As specified in Policy 201.15, all non-student employees are subject to employee criminal background checks.
f. Each employee and student with computer access is issued a unique ID and password. Employees must change passwords periodically using a specific password protocol to minimize the potential of "hacking" and must ensure that all passwords are secured.
g. The College limits access to various computer systems to employees requiring such access for the completion of their job duties.
h. Employees with access to secure student information must implement a keyboard locking protocol to secure information when they are away from their workstations.
i. The College has a system of "permissions" and "controls" in place to limit both inquiry and data entry access to various systems and system components to protect from unauthorized access to confidential information.
j. All data are erased when disposing of computers and other electronic media that contain customer information.
k. Effective disposal of hardware occurs after the completion of its useful life cycle. The College maintains a comprehensive inventory of its technology equipment.
l. Employees with laptops containing sensitive data must follow the protocols in the Secure Laptop Policy (Policy 202.20), including the use of encrypted laptops or thumb drives if secure data are taken off campus.
m. The College's contracted vendor provides assurance that there is effective erasure of all confidential scanned data from photocopiers.
n. The College and/or its contracted vendors ensure that confidential data are maintained and disposed in accordance with state records retention statutes.

2) Physical Safeguards

a. Access to the server room is restricted to certain employees issued electronic key fobs. The room remains locked at all times and has been fortified with additional physical protection.

b. Rooms and/or file cabinets containing paper records with confidential customer information are locked.
c. Fireproof cabinets are used to store student records, financial aid files and employee financial information.
d. All employees are trained to safely dispose of confidential information using shredders or special disposal bins.
e. Any confidential material not shredded on campus is disposed of by a bonded confidential data disposal agency.
f. Confidential materials not housed on campus are stored off-site at a bonded storage company. Records are retained in accordance with federal or state records retention requirements and are destroyed after the retention period.

3) Other Safeguards

a. Financial account information is not provided over the telephone or in-person, unless or until an individual can produce sufficient identification.
b. The College limits employees who may accept financial information (example: credit card numbers) and does not keep permanent records of student financial information.
c. The College outsources payment plan, credit card processing and payroll activities to external vendors and receives assurances from these vendors that they are in compliance with all federal and state mandates.
d. Social security numbers are not used for student identification. Social security information is collected only for federal or state mandated purposes, such as financial aid filing or tax reporting.
e. Signed releases or court-mandated documents are required for the release of FERPA covered information.
f. The College has developed Emergency Action, Disaster Recovery and Business Continuity Plans/Procedures. Offices are responsible for periodically updating these documents.
g. The College's internal controls and operating procedures are reviewed annually by an independent auditing firm.

Approved: 5/20/09
Revised: 2/27/2013
Revised: 9/16/2020

501.6.2 FEDERAL TRADE COMMISSION (FTC) RED FLAGS RULE

The purpose of this section is to define the policies and procedures that Warren County Community College shall follow to be compliant with the FTC Red Flags Rule.

A) Definitions

Under the 2008 FTC Red Flags Rule, any financial agency holding a covered account must develop policies and procedures to detect, prevent and mitigate identity theft.

According to the FTC, a **covered account** includes any account where non-profit and government entities defer payments for goods and services, which includes student payment plans or student loans. For the purposes of Warren County Community College, **a "covered account" refers to transactions related to payments or refunds on student payment plans and disbursements/refunds of federal student loans**.

A **red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

B) Purpose of WCCC's Identity Theft Prevention Program

Warren County Community College is committed to protecting its constituents (including students, faculty and staff) from identity theft. This policy establishes Warren County Community College's Identity Theft Prevention Program ("Program") to detect, prevent and mitigate identity theft. The Program shall include reasonable policies and procedures to:

1) Identify possible relevant red flags that may exist for covered College accounts;

2) Develop procedures to alert employees of relevant red flags;

3) Develop procedures to respond appropriately to red flags that are detected to prevent and mitigate identity theft; and

4) Ensure that the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft.

C) Identification of Relevant Red Flags

As part of the College's efforts to help prevent identity theft, WCCC will consider additional scrutiny and/or follow-up actions when it believes a "red flag" action/activity has occurred. This "red flag" action/activity may include, but is not limited to, events when one or more of the following occur:

1) The College receives notification from a credit agency, governmental agency, law enforcement individual or other source that possible identity theft may be promulgated by or promulgated against a member of the campus community.

2) A campus constituent presents information that may be indicative of possible identity theft, including, but not limited to:

    a) an unexplained address discrepancy
    b) a name discrepancy on identification or insurance documentation
    c) presentation of suspicious documents
    d) presentation of personal information that is inconsistent with information already on file
    e) presentation of inconsistent financial verification documents (e.g., inconsistencies on documentation presented through financial aid or financial payment processes)

f) presentation of a credit card in the name other than the payee with no verifying documentation or permission from the cardholder to use such a document

3) A campus constituent undertakes unusual or suspicious activity related to a campus account. This could include, for example, a request for a financial refund prior to a payment clearing or a pattern of enrolling/dropping of classes prior to the start of the semester.

4) An individual with a prior history of unusual or suspicious payment activity attempts a financial transaction. This could include a "bad check" history with the College or a previous debt balance.

5) Other unspecified actions or account discrepancies that could lead a College official to conclude that identity theft may have been or may be occurring.

For the purposes of this policy, the College will endeavor to apply the "red flag" scrutiny to all student accounts as appropriate, including, but not necessarily limited to, accounts covered through student payment plans and/or student loans (i.e., the accounts required to be monitored under the FTC requirements) until the discrepancy or issue has been resolved.

D) Identification of External "Red Flag" Threats

With the proliferation of telephone, email and text technology, there are constant efforts by parties external to the college to try to obtain data, information or even payments due to students or contractors by fraudulent means, such as impersonating the president and requesting a change in direct deposit, or alleging that they are a government agent and therefore entitled to certain personal information. There are cases where persons representing students, an employee or a contractor has contacted a college or university and asked for a change address for a payment. These efforts, if successful, could result in the redirection of funds to fraudulent accounts. To mitigate such external threats, the College shall do the following:

1) Identify all emails that do not come from the College email system as "EXTERNAL" in the title so employees know that any spoofed email is not from the College.
2) Notify employees if a specific type of campaign seems to be occurring
3) Send out routine information to employees on how they can safeguard their identities and protect themselves and family members from identity theft perpetrators.
4) Remind employees about the appropriate ways that information can be changed (forms, etc.) rather than through e-mail.
5) If information is coming from a common address, WCCC can block that address.
6) Contact external agencies (including federal fraud agencies) when a specific campaign appears to be targeting the college.

E) Institutional Response

An individual suspecting that a red flag has been triggered shall notify the Vice President of Finance and Operations or his/her designee of concerns. The concern shall be promptly investigated by the College. The College's response to such "red flag(s)" shall be commensurate with the degree of risk imposed. Depending on the circumstance(s) and the severity of the action/activity, the College may

consider one or more of the following after encountering a "red flag" circumstance. The possible actions of the Vice President or designee shall be as follows:

1) Determine that no response is warranted under the specific circumstances;

2) Require additional/confirming information or identification from an individual before processing the transaction;

3) Attempt to contact the account holder if he/she is not present in person to verify a transaction;

4) Deny the processing of any transaction until or when any discrepancy or issue is cleared;

5) Place a "hold" on a student account so that no further transactions can occur until the discrepancy or issue is cleared. This hold shall act to notify other campus offices of a financial issue with the account;

6) Discontinue any student access to an account (e.g., change password or deny on-line access)

7) Contact any appropriate financial agency regarding an account discrepancy (this may include a payment plan provider, student loan vendor, credit card holder or credit reporting agency)

8) Notify relevant federal or state agencies/authorities regarding information discrepancy (such as the National Student Loan Clearinghouse, Federal Department of Education or the NJ Higher Education Student Assistance Authority);

9) Forward concerns to the President, who will consider whether there has been a violation of the campus code of conduct or other policies and who shall be responsible for notifying other campus officials, including the Board of Trustees, as appropriate, of such an incident; and/or

10) Contact local law enforcement if it appears that a criminal activity may have occurred.

F) Responsibilities for Implementation, Review and Update of Program

1) The College shall charge the Vice President, Finance and Operations for overseeing initiatives to safeguard the financial information of constituents served by the College.

2) In addition to overseeing internal safeguards, the Vice President, Finance and Operations shall exercise appropriate and effective oversight of service provider arrangements and receive assurances that that they are in compliance with Red Flags Rule (example: Payment Plan, Bookstore vendors).

3) The College shall investigate instances where possible identity theft is occurring and report such issues to external agencies, including local law enforcement, as appropriate.

4) The College's Committee on Finance and Audit shall review compliance issues as part of the annual financial audit of the College and update the Program to reflect changes in statutes, industry practice or campus experience related to identity theft.

Approved: 5/20/09
Revised: 2/27/2013
Revised: 09/16/20

405 Distance Education

Distance Education credit courses shall be defined as courses that rely on technology to deliver course content when the learner and instructor are not in the same place at the same time. Distance Education courses may be synchronous (in real time; simultaneous) or asynchronous. Distance education is distinct from hybrid courses, where the instructor and students have a regular meeting schedule (usually once a week) but rely on technology to deliver a portion of the course content.

Also, in accordance with Federal Regulations, the College must establish procedures to ensure the identity of each student taking distance education classes. These procedures are intended not only to protect student privacy, but to also prevent any academic misconduct. WCCC satisfies this requirement through the following controls:

a) Students and instructors are only permitted access to classes for which they are enrolled.
b) Users must submit both a unique user ID and a password in order to access their distance education classes.
c) Instructors or academic administrators can monitor student use and disable a user's access to a class in the case of any suspected violation of academic policies or procedures.
d) An instructor may specify in-person assessment(s) for distance education or hybrid courses, as long as these requirements are made clear in the section syllabus. All in-person assessments must be proctored by the instructor or an authorized college representative. No additional fees shall be charged to students for the proctoring of distance education or hybrid course assessments.

The college shall verify that a student is actively attending a distance education course prior to the disbursement of federal financial aid. Because distance education courses do not include face-to-face contact between a professor and a student, it is necessary for the college to establish standards for determining attendance for purposes of financial aid disbursement. Attendance in on-line class shall be defined as active participation in course assignments, including the completion of papers, on-line postings and exams. Merely logging into an on-line educational system **does not** constitute attendance.

Students enrolled in a distance education class who have not completed a single course assignment/exam for the class, shall receive an NF grade (Failure to Withdraw/Never Attended). Students who have stopped actively participating in the class prior to the end of the semester shall be awarded an XF grade (Failure to Withdraw/Stopped Attending) and have a "last date of attendance" (or LDA) date recorded by the instructor. This LDA shall reflect the date the student's last assignment or exam was received by the instructor.

Any instructor or administrator concerned about the sharing, tampering or access to usernames, passwords, or distance education courses by unauthorized individuals shall report concerns

immediately to the Vice President of Academic or his/her designee. This includes concerns regarding possible student fraud, plagiarism and/or other conduct specifically prohibited in the Student Handbook, the Campus Code of Conduct (Policy 304.2), the Policy on Computer, Email and Internet Usage (Policy 202.19) or the Copyright Policy (Policy 404).

It is the responsibility of the instructor to utilize the course objectives and the defined textbook as set forth in the master syllabus for all distance education courses. The college approved Learning Management System (LMS) must be utilized for all distance education courses and may be supplemented with additional online resources as approved by the college administration. Distance education courses must also meet guidelines established by the college for student time on task. A guideline of proposed time must be pre-approved by the Vice President of Academics before the start of the academic term. Each week faculty must document attendance within the LMS on all students enrolled in distance education courses. A final time audit reflecting actual course structure and student time on task must be submitted to the Vice President of Academics at the conclusion of the course along with final grades and attendance information.

Approved 6/29/2011
Revised 2/27/2012
Revised 2/26/2014
Revised 6/24/2015
Revised 11/7/18

404 Copyright Policy

Warren County Community College shall comply with the 1976 Copyright Act through the following guidelines and standards of educational fair use as specified under Section 107 of H.R. 2223.

404.1 GUIDELINES FOR CLASSROOM COPYING WITH RESPECT TO BOOKS AND PERIODICALS

I. Single Copying for Teachers

A single copy may be made of any of the following by or for a teacher at his or her individual request for his or her scholarly research or use in teaching or preparation to teach a class:

A. A chapter from a book;
B. An article from a periodical or newspaper;
C. A short story, short essay or short poem, whether or not from a collective work;
D. A chart, graph, diagram, drawing, cartoon picture from a book, periodical, or newspaper;

II. Multiple Copies for Classroom Use

Multiple copies (not to exceed in any event more than one copy per pupil in a course) may be made by or for the teacher giving the course for classroom use or discussion; provided that:

A. The copying meets the tests of brevity and spontaneity as defined below; and,

B. Meets the cumulative effect test as defined below; and,
C. Each copy includes a notice of copyright

DEFINITIONS:

Brevity:

1. Poetry
    a. A complete poem if less than 250 words and if printed on not more than two pages or,
    b. from a longer poem, an excerpt of not more than 250 words.

2. Prose
    a. Either a complete article, story or essay of less than 2,500 words, or
    b. an excerpt from any prose work of not more than 1,000 words or 10% of the work, whichever is less, but in any event a minimum of 500 words.

    [Each of the numerical limits stated in 1 and 2 above may be expanded to permit the completion of an unfinished line of a poem or of an unfinished prose paragraph.]

3. Illustration: One chart, graph, diagram, drawing, cartoon or picture per book or per periodical issue.

4. "Special" works: Certain works in poetry, prose or in "poetic prose" which often combine language with illustrations and which are intended sometimes for children and at other times for a more general audience fall short of 2,500 words in their entirety.

    Paragraph 2 above notwithstanding such "special works" may not be reproduced in their entirety; however, an excerpt comprising not more than two of the published pages of such special work and containing not more than 10% of the words found in the text thereof, may be reproduced.

Spontaneity:

1. The copying is at the instance and inspiration of the individual teacher, and

2. The inspiration and decision to use the work and the moment of its use for maximum teaching effectiveness are so close in time that it would be unreasonable to expect a timely reply to a request for permission.

Cumulative Effect:

1. The copying of the material is for only one course in the school in which the copies are made.

2. Not more than one short poem, article, story, essay or two excerpts may be copied from the same author, nor more than three from the same collective work or periodical volume during one class term.

3. There shall not be more than nine instances of such multiple copying for one course during one class term.

   [The limitations stated in 2 and 3 above shall not apply to current news periodicals and newspapers and current news sections of other periodicals.]

III. PROHIBITIONS TO I AND II ABOVE

Notwithstanding any of the above, the following shall be prohibited:

A. Copying shall not be used to create or to replace or substitute for anthologies, compilations or collective works. Such replacement or substitution may occur whether copies of various works or excerpts therefrom are accumulated or reproduced and used separately.

B. There shall be no copying of or from works intended to be "consumable" in the course of study or of teaching. These include workbooks, exercises, standardized tests and test booklets and answer sheets and like consumable material.

C. Copying shall not:
   1. substitute for the purchase of books, publishers' reprints or periodicals;
   2. be directed by higher authority;
   3. be repeated with respect to the same item by the same teacher from term to term.
   4. No charge shall be made to the student beyond the actual cost of the photocopying.

404.2 GUIDELINES FOR CLASSROOM COPYING WITH RESPECT TO MULTIMEDIA WORKS

Creators of multimedia products for course-related work may prepare a total of three copies, one of which is for preservation and replacement purposes only. One of the copies may be placed on Library Reserve. Fair Use status expires two years after the first instructional use of a particular multimedia product.

Multimedia products should contain an opening screen notice that credits the sources, displays the copyright notice and copyright ownership information if shown in the original source. Crediting the source must adequately identify the source of the work, giving a full bibliographic description where available. The copyright notice includes the word "Copyright" or the copyright symbol, the name of the copyright holder, and the year of first publication. Any alterations of copyrighted items must be noted.

There are quantitative portion limitations that specify how much of copyright protected sources may be included in multimedia products prepared by students or faculty for course-related work. Use of larger portions requires permission from copyright owners.

1. Text
   Up to 10% or 1000 words of a source, whichever is less. An entire poem of less than 250 words, but no more than 3 poems or excerpts by one poet. No more than 5 poems or excerpts from one anthology.

2. Music, Lyrics, Music Video
   Up to 10% but not more than 30 seconds total from an individual work

3. Motion Media
   Up to 10% or 3 minutes of a source, whichever is less.

4. Illustrations, Photographs
   No more than 5 images by one artist or photographer. No more than 10% or 15 images, whichever is less, from any single published work.

5. Numerical Data Sets
   Up to 10% or 2500 fields or cell entries, whichever is less.

6. Internet Sources
   Though it can be difficult to determine what is copyright protected and what is in the public domain, the multimedia creator is responsible for adhering to copyright law.

7. Opening screen notice
   "Certain materials are included under the fair use exemption of U.S. Copyright Law and have been prepared according to the educational multimedia fair use guidelines and are restricted from further use."

404.3 USE OF TORRENT OR SIMILAR PROTOCOL TO DOWNLOAD COPYRIGHTED MATERIALS

BitTorrent is an information technology protocol that allows peer-to-peer file sharing that is used to distribute large amounts of data over the Internet. Over the past several years, the use of BitTorrent and similar software has been used to illegally download and share copyrighted media, especially movies and premium cable television offerings. The use of BitTorrent or similar software to download copyrighted material on the WCCC campus is considered a violation of the College's technology, code of conduct and copyright policies. Individuals who illegally download materials shall be subject to discipline by the College in addition to any externally imposed legal penalties.

404.4 SUMMARY OF CIVIL AND CRIMINAL PENALTIES FOR VIOLATION OF FEDERAL COPYRIGHT LAWS

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement. Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505. Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please see the website of the U.S. Copyright Office at www.copyright.gov.

Approved: 09/08/10
Revised: 05/17/14
Reaffirmed: 05/18/2019