Wharton County Junior College	ADMINISTRATIVE PROCEDURE MANUAL	
WCJC Title: **Technology Resources (CR)**	Section C: **Business and Support Services**	Page(s): 6
BASED ON BOARD OF TRUSTEES POLICY		
Policy Title: **Technology Resources**	Policy: CR (Local)	
Subtitle: None	Date Adopted: 8-01-20	

Purpose

Describes rules governing the users of Wharton County Junior College's (WCJC) technology resources.

Procedure

Availability of Access

Access to the WCJC's technology resources are primarily for educational purposes and for the conduct of college business; but the College does not prohibit the personal use, with certain restrictions specified herein, of these resources and services.

The College reserves the right to restrict the use of or permanently disconnect any wireless device from the campus network if that wireless device disrupts or interferes with services provided by the College, or behaves in such a way that the service or security of College Technology Resources is impacted.

The WCJC wireless network is intended as a supplement to the wired network and for use with portable electronic devices; it is not intended to be a user's sole connection to the College network or Technology Resources. The wireless network should not be expected to provide the same quality of service as the College's wired network infrastructure. When reliability and performance are critical, the College's wired network infrastructure should be used. Stationary computing devices, such as PC towers, printers, servers, and other critical Technology Resources such as research equipment must be connected to WCJC's wired network infrastructure where reasonably possible.

Acceptable Use

In using the College's computer and telecommunications resources and electronic communication services, the individual users thereby agree to abide by the College's

policies and procedures. They also acknowledge that any violation of this regulation is unethical, may constitute a criminal offense, and may result in suspension or revocation of access privileges, other disciplinary action including dismissal, and/or legal action.

System users and parents of students with access to the College's system should be aware that the use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

1. The following procedures are the responsibility of all deans, division chairs, department heads, and supervisors:

    a. Insure that employees within a department receive opportunities to attend training courses that help them to comply with this policy and other applicable college policies.

    b. An IT Help Desk ticket will be promptly submitted when employees have been separated so that the separated employee's access to College computer resources may be disabled.

    c. Promptly report ongoing or serious problems regarding computer use to the office of Vice President of Technology in a detailed written communication.

2. The following actions are responsibilities of all users:

    a. Users are required to acknowledge receipt and understanding of all administrative regulations governing use of WCJC's technology resources. A copy of the WCJC Acknowledgements to Policies form is kept in the employee's personnel file.

    b. Users should have no expectation of personal privacy with respect to WCJC technology resources and understand that technology resources may be monitored for, but not limited to, managing performance, performing routine maintenance and operations, protecting the integrity of WCJC technology resources, performing security reviews, and fulfilling investigation requirements.

    c. Users are to use College computer resources responsibly, respecting the needs of other computer users.

    d. Users are responsible for any usage of their computer account. Users shall maintain the secrecy of their password(s).

    e. Users are to report any misuse of computer resources or violations of this policy to their supervisors or to the Vice President of Technology. Students are to report suspicious computer activity to a college employee.

f. Users are to comply with all reasonable requests and instructions from the Information Technology Department.

g. When communicating with others via the College computer system, users' communications are to reflect high ethical standards, mutual respect, and civility.

h. Employees are required to follow the Office of Marketing and Communications procedures for publishing a signature line as part of their WCJC email account. These procedures can be found on the WCJC Marketing and Communications Intranet page called Email Signature Guidelines.

i. Users are to comply with all software licenses, copyrights, and all other state and federal laws governing intellectual property.

j. Users are to exercise the same care and discretion in drafting e-mail and other electronic documents as they do in any other written communications.

k. Users may not alter or copy a file created by another user without first obtaining permission from the owner or custodian of the file. The ability to read, alter, or copy a file created by another user does not imply permission to read, alter, or copy that file. Similarly, a user's ability to connect to other computer systems through the College's network does not imply a right to do so or to make use of those systems.

l. Users who identify a security problem in the College's system are to immediately notify the office of Vice President of Technology in a detailed written communication.

3. The failure to follow procedures is also known as a deliberate act. The following actions constitute misuses of the College computer resources and are strictly prohibited for all users:

a. Use of e-mail or other forms of electronic communication for, or the display of, or the storage of fraudulent, harassing, embarrassing, indecent, profane, obscene, intimidating, inaccurate, sexually explicit, threatening, offensive, or other unlawful material. Users encountering or receiving such material are to immediately report the incident to a supervisor.

b. Abuse of computer resources including, but not limited to, any act that endangers or damages specific computer software, hardware, program, network or the system as a whole, whether located on campus or elsewhere on the global Internet; creating or purposefully allowing a computer malfunction or

interruption of operation; intentional injection of a computer virus onto the operations of outside entities; printouts that tie up computer resources for an unreasonable time period; and failure to adhere to time limitations that apply at particular computer facilities on campus.

c. Use of College computer resources for personal financial gain or a personal commercial purpose is not permitted. College resources may not be used for the transmission or storage of personal advertisements, solicitations, and promotions; destructive programs (viruses and/or self-replicating code); political material; or any other unauthorized use.

d. Failure to protect a password or account from unauthorized use, which may result in student suspension and/or employee termination. The user in whose name a system account is issued is responsible at all times for its proper use. Individual passwords are not to be stored online, or given to others. Users are responsible for all transactions made using their passwords.

e. Unauthorized access or reading of any electronic file, program, network, or the system.

f. Unauthorized use, duplication, disclosure, alteration, damage, or destruction of data contained on any electronic file, program, network, or College hardware or software.

g. Unauthorized duplication of commercial software. All commercial software is covered by a copyright of some form. Duplication of software covered by such copyrights is a violation of the copyright law and this policy.

h. Attempting to circumvent, assisting someone else or requesting that someone else circumvent, any security measure or administrative access control that pertains to College computer resources.

i. Use of College computer resources to encourage the use of alcohol or other controlled substances or to otherwise promote any other activity prohibited by College policy or state or federal law.

j. Use of the College computer resources in a manner that violates other College policies such as those prohibiting racial, ethnic, religious, sexual, or other forms of harassment.

k. Forgery or attempted forgery of electronic-mail messages. Attempts to read, delete, copy, or modify the electronic mail of other system users; to interfere deliberately with the ability of other system users to send or receive electronic

mail; or to use another user's name, log-on ID, or password to send or receive messages are prohibited.

4. Any attempt to harm or destroy College equipment or materials, data of another user, or any of the networks or agencies that are connected to the Internet or the College's intranet is prohibited. Deliberate attempts to degrade or disrupt system performance are viewed as violations of college policy and procedures and may be viewed as criminal activity under applicable state and federal laws. Violations include, but are not limited to, uploading or creating of computer viruses and the use of any software having the purpose of damaging the College's system or other systems, also known as malware.

5. The College assumes no responsibility or liability for any membership or charges including, but not limited to, long-distance charges, per-minute (unit) surcharges, bandwidth, and/or equipment or line costs incurred by home usage of the College's system resources. Further, any disputes or problems regarding services for home users of the College's system are strictly between the user and his/her service provider.

6. Failure to adhere to the provision of this regulation may lead to cancellation of a user's computer account(s), suspension, dismissal, or other disciplinary action by the College, as well as referral to legal and law-enforcement agencies.

    a. The College may suspend or revoke a user's access to the system upon any violation of any part of this regulation.

    b. A system user may appeal the suspension or revocation of access or other disciplinary action by invoking the procedures in the applicable complaint, grievance, or appeal process.

Monitored Use

The College has the right, but not the duty, to monitor any and all aspects of the computer system, including email, to ensure compliance with CR (Legal) and CR (Local). All non-copyrighted data stored on the College's computer resources are the property of the institution.

Disclaimer of Liability

The College's system is provided on an "as-is, as-available" basis. The College does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by or through the system and any information of software contained therein. The College does not warrant that the functions or services performed by the system or the information of software contained on the system will meet the user's requirements or expectations; nor

does the College warrant that the system will be uninterrupted or free of error or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of those parties and not of the College.

The College will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the College's electronic communications system.

Record Retention

Refer to CIA (Local).

Access by Individuals with Disabilities

Students with disabilities are encouraged to inform the college of any assistance they may need by following the Steps to Apply for Accommodations located on the WCJC website at https://wcjc.edu/About-Us/administration/offices/student-services/disability-services.aspx

Drones

Refer to CR (Legal).

Date Prepared: 7-12-21 (PY)

Revised date: