REGULATIONS

REG No.: 146

COMPUTER USE

I. PURPOSE

Describes rules governing the use of computer resources and electronic communications. The purpose of this regulation is to insure proper use of the college's computer and telecommunications resources and electronic communication services by its students, employees, and other computer users.

II. BACKGROUND and/or LEGAL REFERENCES

All computer users have the responsibility to use computer resources in an efficient, effective, ethical, and lawful manner.

This regulation applies to all users of college computer, wireless network, learning management system and telecommunications resources and services, wherever the users are located. Violations of this regulation may result in disciplinary action, including possible termination and/or legal action.

The college has the right, but not the duty, to monitor any and all aspects of the computer system, including e-mail, to insure compliance with this regulation. All non-copyrighted data stored on the college's computer resources are the property of the institution.

As with any private device connected to the campus network, 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 IT Resources is impacted.

Computers, computer and learning management system access and computer accounts given to employees and students 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 following references are relevant to this topic:

Texas Penal Code, Chapter 33: Computer Crimes. Unauthorized use of college computers or unauthorized access to stored data or dissemination of passwords or other confidential information to gain access to the college's computer system or data is in violation of state criminal law.

Texas Penal Code, Chapter 37: Tampering with Governmental Records. Any alteration, destruction, or false entry of data that impairs the validity, legibility, or availability of any record maintained by the college is a violation of state criminal law.

U.S. Penal Code, Title 18, Section 1030: Fraud and Related Activity in Connection with Computers. Among other stipulations, prohibits unauthorized or fraudulent access.

Federal Copyright Law, Title 17, Section 106. Recognizes that all intellectual works are automatically covered by copyright. The owner of a copyright holds exclusive right to reproduce and distribute the work.

Computer Fraud and Abuse Act of 1986. Makes it a federal crime to access a computer to obtain restricted information without authorization; to alter, damage, or destroy information on a governmental computer; and to traffic in passwords or similar information used to gain unauthorized access to a government computer.

Electronic Communications Privacy Act of 1986. Prohibits interception or disclosure of electronic communication, and defines those situations in which disclosure is legal.

Computer Software Rental Amendments Act of 1990. Prohibits the unauthorized rental, lease, or lending of copyrighted software.

III. DEFINITIONS

A. Computer *resources* include hardware, software, internal and external communications networks, electronic storage media, cloud storage, manuals, and other documentation. Computer, wireless access points and telecommunications services include, but are not limited to, computers (networked, stand- alone, laptops, tablets, etc.), file servers, smartphones, e-mail, online services, portal services, bulletin-board services, etc., that are accessed directly or indirectly from the college's computer facilities.

B. *Data* includes all files, regardless of size or storage media, including e-mail messages, system logs, and software (whether commercially or locally developed).

C. *Users* includes all students, employees, independent contractors, and other persons or entities accessing or using the college's computer and telecommunications resources and services.

D. A *Learning Management System* (LMS) refers to the software application for the administration, documentation, tracking, reporting and delivery of distance education courses. The LMS can also be utilized to supplement instruction in traditional face-to-face courses.

E. The 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 IT 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 IT Resources such as research equipment must be connected to WCJC's wired network infrastructure where reasonably possible.

IV. POLICY

A. The college shall have standard procedures for the use of computer resources, including a delineation of appropriate and inappropriate use of information technology resources.

B. *Authorized Use.* The college shall provide computer resources for the purpose of accomplishing tasks related to the college's mission.

C. *Students.* Students shall be allowed to use the college’s computer resources for school-related purposes in computer class rooms and personal purposes in designated open computer labs and the College’s wireless network. Utilization is subject to this regulation and other applicable college policies, state and federal law, and as long as personal use does

not result in any additional costs to the college or endangerment to IT equipment and network.

D. *Employees.* An employee of the college shall be allowed to use computer resources in accordance with this and other applicable college policies. Incidental personal use of computer resources by employees is permitted subject to review and reasonable restrictions by the employee's supervisor, adherence to applicable college policies and state and federal law, and as long as such usage does not interfere with the employee's accomplishment of his or her job duties and does not result in any additional costs to the college or endangerment to IT equipment and network. When an employee terminates employment, his or her access to the college's computer resources is terminated immediately.

E. *Freedom of Expression.* The college shall not limit access to any information due to its content as long as such access is legal and as long as the college's computer resources are not used for inappropriate purposes including but not limited to pornographic, harassment, or threatening purposes. The college reserves the right to place reasonable time, place, and manner restrictions on freedom of expression on its computer resources.

F. *Privacy.* Computer use shall be subject to review or disclosure in accordance with the Texas Public Information Act and other laws, administrative review of computer use for security purposes or in regard to a policy or legal compliance concern, computer system maintenance, audits, and as otherwise required to protect the reasonable interests of the college and other users of the college's computer resources. Anyone using the college's computer resources expressly consents to monitoring on the part of the college for these purposes and is advised that if such monitoring reveals possible evidence of criminal activity, college administration may provide that evidence to law-enforcement officials. Further, the college does not guarantee the protection of electronic files, data, or e-mails from unauthorized or inappropriate access.

G. *Intellectual Property.* Intellectual property laws extend to the electronic environment. Users shall assume that works communicated through the computer network are subject to copyright laws, unless specifically stated otherwise.

H. *Valuable Assets.* Computer resources and data are considered valuable assets of the college. Further, computer software purchased or leased by the college is the property of the college or the company from whom it is leased. Any unauthorized access, use, alteration, duplication, destruction, or disclosure of any of these assets may constitute a computer- related crime, punishable under Texas statutes and federal laws. College computer resources may not be transported or relocated without appropriate authorization.

I. *Criminal and Illegal Acts.* College computer resources shall not be used in support of or for illegal activities. Any such use shall be reported and dealt with by the appropriate college authorities and/or law-enforcement agencies. Criminal and illegal use may involve, but is not limited to, unauthorized access, intentional corruption or misuse of computer resources, theft, obscenity, and child pornography.

(POLICY APPROVAL: 8-15-99, Board of Trustees, amended 10-18-11, amended 10-16-12, amended 10-18-16)

V. PROCEDURES

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

1. 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.

2. 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.

3. Promptly report ongoing or serious problems regarding computer use to the office of Vice President of Technology/IR.

B. The following actions are responsibilities of all users.

1. Users are to use college computer resources responsibly, respecting the needs of other computer users.

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

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

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

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

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

7. 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.

8. 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.

9. Users who identify a security problem in the college's system are to notify the Information Technology Department.

C. 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:

1. 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.

2. 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.

3. 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.

4. 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.

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

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

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

D. 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.

E. 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.

F. 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.

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

2. 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 regulation: Reg 591, Student Grievances; Reg 664, Appeal of Student Disciplinary Action; Reg 877, Employee Grievances and Complaints.

VI. GUIDELINES

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.

VII. DISCLAIMER

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.

VIII. USER AGREEMENT

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.

RMP/BAM/FRV
8-15-99
PY/BM
10-18-11
PY/BM
10-16-12
PY/BM
7-15-14
PY
4/13/16

Reg. 146