EL PASO COMMUNITY COLLEGE PROCEDURE

For information, contact Institutional
Effectiveness: (915) 831-6740

CR-2 **Acceptable Use of Information Technology Resources**

APPROVED: July 18, 2005 **REVISED**: May 1, 2019
Year of last review: 2021
AUTHORIZING BOARD POLICY: CR

Classification: Administrative
Responsible Vice President or Associate Vice President: Vice President of Information Technology/CIO
Designated Contact: Vice President of Information Technology/CIO

OBJECTIVE: To establish the requirements for the use of all technology, computing, and network resources at El Paso Community College (EPCC).

PROCEDURE:

I. Access to Information Technology Resources

A. A user is defined as anyone who uses EPCC technology or technology on behalf of EPCC, whether it is used locally or remotely, including, but not limited to, all EPCC faculty, staff, students, visitors, contractors, consultants, and anyone who connects to or uses EPCC systems or networks (users). All users are required and presumed to know and comply with all applicable laws, policies, and rules governing the use of EPCC technology.

B. EPCC technology includes all College-owned, licensed, or managed hardware, including, without limitation, servers, desktop computers, laptop computers, tablet devices, mobile phones or other mobile web-enabled devices, telephones, and facsimile machines, software, data files, network drives, communications systems, and any data transferred through the College's physical or wireless network, regardless of ownership or affiliation.

C. EPCC technology also includes any and all technology administered or developed by anyone employed by or representing the College, including all applications, data, and services (e.g., web sites and software developed for or representing EPCC and its constituents).

II. Acceptable Use Requirements

A. Users may only utilize and/or access EPCC technology for which they have the proper authorization.

B. Users will make every effort to protect their login name and passwords and to otherwise secure EPCC technology against unauthorized access, including enabling and utilizing security features on all computers, mobile phones, tablets, and other devices.

C. Users may not use or attempt to gain access to another user's EPCC technology or attempt to obtain another user's credentials.

D. Each user is personally responsible for the appropriate use of all EPCC technology assigned to the user or to which the user has authorized access.

E. Users will be accountable for any misuse or unauthorized access of the EPCC technology assigned to them. Users may not enable unauthorized persons to access the EPCC network by using an EPCC computer or a personal computer that is connected to the EPCC network. Any such misuse or unauthorized access may result in disciplinary action for the user.

F. Users are expected to comply with all contractual and licensing agreements respecting certain third-party resources by which EPCC is bound.

G. Users must comply with any additional requirements, policies, or guidelines established for specific EPCC technology to which the user has been granted access. When additional requirements, policies, and

guidelines are more restrictive than this procedure, the more restrictive requirements, policies, or guidelines will take precedence.

H. Users must not install or use EPCC technology in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software, or hardware components of a system.

I. If an EPCC user uses a personally owned device to access EPCC technology or conduct EPCC business, he or she shall abide by this procedure and all other applicable EPCC policies and administrative procedures. Users should be aware that any use of a personally owned device may subject the contents of that device and any communications sent or received on it to disclosure pursuant to a lawful subpoena or open records request.

J. In addition to the above mentioned general requirements, the following specific uses of EPCC technology are clearly prohibited:

1. Use of a non-EPCC-issued email service or online storage service for conducting EPCC business unless use of the non-EPCC service has been expressly authorized in writing by EPCC's Vice President Information Technology or his or her designee;

2. Sharing one's assigned online services account information, passwords, or other information used for identification and authorization purposes;

3. Developing or establishing Internet technologies and services that serve or represent EPCC without proper authorization or in violation of other EPCC policies and regulatory requirements;

4. Accessing, posting, displaying, transmitting, or otherwise using material that is discriminatory, defamatory, obscene, sexually explicit, harassing, intimidating, threatening, or disruptive;

5. Disclosing or in any way causing to be disclosed confidential or sensitive College, employee, or student information;

6. Engaging in personal commercial or other for-profit activities;

7. Using EPCC technology for personal political activity or to engage in political lobbying on behalf of EPCC;

8. Infringing on copyright, license, trademark, patent, or other intellectual property rights;

9. Intentionally disrupting or harming EPCC technology or other College operations, including, without limitation, destroying College equipment, placing a virus on College computers, adding or removing a computer program without authorization, changing settings on shared computers without authorization, or removing data from EPCC technology without authorization;

10. Installing or using unauthorized software on EPCC technology;

11. Storing EPCC records in any form in an unsecured or unapproved location, or on an unsecured or unapproved system;

12. Violating any EPCC Board policy or administrative procedure;

13. Gaining unauthorized access to the data files or equipment of others, accessing electronic resources by using another person's name or electronic identification, or sending anonymous electronic communications;

14. Engaging or promoting in any activity that is illegal under local, state, federal or international law while utilizing EPCC owned technology resources;

15. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, copyrighted movies, and the installation of any copyrighted software for which the end user does not

have an active license is strictly prohibited;

16. Accessing data, a server or an account for any purpose other than conducting EPCC business, even if you have authorized access, is prohibited;

17. Circumventing user authentication or security, including, but not limited to, any host, network or account.

18. Users may not attempt to bypass computer or network security mechanisms, including the EPCC Network, without the prior express permission by Information Technology. Possession of tools that bypass security or probe security, or of files that may be used as input or output for such tools, shall be considered as the equivalent to such an attempt. The unauthorized scanning of the EPCC Network is prohibited.

III. Privacy and Monitoring

A. While the College recognizes the importance of privacy in an institution of higher learning and will endeavor to honor that ideal, users should have no expectation of privacy in any information stored on or sent through EPCC technology or personal devices connected to EPCC technology, except as required by law. Users should note that electronically stored information of any kind may be discoverable in a legal action or accessed and reviewed during the course of an EPCC administrative investigation.

B. All EPCC technology including, but not limited to, equipment, and the work, data, and other material stored on it in any form is subject to review, monitoring, blocking, or removal by EPCC, as well as other maintenance and protective actions, such as logging, deleting, encrypting or decrypting, threat analysis, performance analysis, backup, and troubleshooting. All such actions are within the authority of EPCC's administration.

C. Authorized users must not violate the privacy of other users. Technical ability to access unauthorized resources or others' accounts does not by itself imply authorization to do so, and it is a violation of this policy to access others' accounts unless authorized to do so for a legitimate business purpose.

IV. Record Retention and Destruction

A. Any electronically stored information generated or received by an EPCC employee which constitutes an EPCC or EPCC-student record shall be classified, retained, and destroyed in accordance with College Procedures 7.08.02.26, *Retention Schedule for Student Educational Records* and 2.01.11.10, *Records Management* which address the retention of College or student records. In addition, all EPCC records must be maintained in an approved repository within the College's jurisdiction.

B. Storing EPCC and EPCC-student records in any medium on unsecured or unapproved systems is a violation of EPCC policy as defined in College Procedures 7.08.02.26, *Retention Schedule for Student Educational Records* and 2.01.11.10, *Records Management*.

V. Data Security and Classification

It is the responsibility of the applicable data custodian to evaluate and classify data for which he/she is responsible according to the classification system adopted by the College.

VI. Reporting Violations

A. Any person who violates this procedure is subject to disciplinary action, to include removal of computer or technology resources access.

B. Any person reporting a violation of this procedure shall contact the appropriate supervisory personnel, who will advise the Vice President, Information Technology/CIO. The Vice President, Information Technology/CIO will inform the College police department as deemed necessary.

VII. Disciplinary Action

Disciplinary action related to violations of this procedure shall be taken in accordance with existing College disciplinary policies and procedures. Disciplinary action could include removal of computer technology resource

access and/or any of the following:

A. For Employees: Unauthorized use or abuse of EPCC technology by EPCC employees may result in disciplinary action.

B. For Students: Use of EPCC technology is subject to the Student Code of Conduct. Unauthorized use or abuse of EPCC technology by EPCC students may result in disciplinary action.

C. For All Users: The misuse or abuse of EPCC technology may also violate state or federal law and may result in additional civil or criminal liability and/or penalties.

VIII. Legal Standards

All users of EPCC technology are expected to abide by all Federal and State laws and regulations. The following list of relevant statutes is used for illustrative purposes, and is not intended to be a comprehensive guide to Federal and/or State law:

A. FERPA (Family Educational Rights and Privacy Act): regulates the confidentiality of student records.

B. GLBA (Graham Leach Bliley Act): regulates the confidentiality of financial information.

C. HIPAA (Health Insurance Portability and Accountability Act): regulates the security and privacy of heath information.

D. PCI DSS (Payment Card Industry Data Security Standard): regulates the confidentiality of credit card information.

E. DMCA 1998 (Digital Millennium Copyright Act): regulates the protection of intellectual property.

F. USC Title 18 §1030 (United States Code: Fraud and related activity in connection with computers)

G. Texas Government Code CHAPTER 552. PUBLIC INFORMATION

H. Texas Administrative Code (TAC) Chapter 202.Subchapter C. Information Security Standards for Institutions of Higher Education.