

Acceptable Use Policy

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

**CQ
(LOCAL)**

PHILOSOPHY AND PURPOSE

The District provides network and Internet access to electronic mail, databases, libraries, museums, and other information sources for the following limited purposes:

1. Promote educational excellence in its schools by facilitating resource sharing, innovation, and communication.
2. Improve learning and reach the District's instructional goals.
3. Achieve effective and efficient administration at the District and campus levels.
4. Comply with the Texas Education Agency's guidelines for technology in schools.

Any use of the District's electronic information systems and resources by authorized users must be in furtherance of these limited purposes and conform to the District's expectations for legal, efficient, and ethical use.

INTERNET SAFETY AND LIMITATIONS ON SITE ACCESS

Recognizing that the Internet can give access to sites containing information that is obscene, child pornography, or harmful to minors or that would be otherwise inappropriate for distribution to students, unsuitable for use in the approved curriculum, or irrelevant to accomplishing the District's stated purposes for operating an Internet-accessible network, the District has installed technology protection measures to filter, screen, analyze, and block site content in an effort to make it more difficult for students or staff to gain access to such material through the District's network.

The technology director or designated campus administrators may disable technology protection measures during use by an adult to allow access to otherwise prohibited or blocked sites or information for bona fide research or other acceptable purposes under this policy.

DATE ADOPTED: August 13, 2007

1

CQ (LOCAL)-X

Nonetheless, the District makes no representation that it can control access to all inappropriate Internet sites. Network users are responsible for their actions in accessing available resources and shall be held accountable for receiving information that is inconsistent with the requirements for acceptable and unacceptable use of the network and Internet.

AUTHORIZED USERS

The District permits individuals in the following categories to become authorized users of its computer network and/or have access to the Internet, subject to administrative regulations developed by the technology director and approved by the Superintendent.

1. Campus administrators and campus administrative support employees.
2. Central office administrators (department or division directors) and their administrative support employees.
3. Instructional personnel.
4. Instructional support and student services personnel, i.e., librarians, counselors, and school nurses.
5. All Cameron ISD students may have access to the network and internet through class accounts and/or individual accounts. All accounts must have principal approval.

All persons, groups, or entities requesting a connection to or the use of the District's computer network are required to have prior permission from the technology department. To become an authorized user, a person must complete an application, sign the user agreement form, and return both forms to the technology director or designee. Minor students applying for a user account must also return a signed parent agreement form. Permission shall be granted on the basis of need, responsibility, liability, security, and compliance to network standards of the District.

GENERAL REQUIREMENTS FOR NETWORK AND INTERNET USE

Student and employee use of the District's computer network and/or access to the Internet must be in accordance with this policy. All persons, groups, or entities shall have approval from the technology department in order to obtain a connection to or the use

of the District computer network. Approval shall be granted on the basis of need, responsibility, liability, security, and compliance with the network standards of the District.

No account sharing shall be permitted, and each authorized user shall be responsible for all activities, transmissions, or actions that occur under that account identifier.

All computers, servers, and any other devices that are connected to the District computer network shall have installed and running a current version of anti-virus software that is approved by the Technology department.

Any user who identifies a security problem with the network must immediately notify the District technology director and may not communicate the problem to any other person.

MONITORING USE

Use of a personal network account through the District's system is voluntary and constitutes a privilege provided by the District, not a right. All network usage is subject to monitoring, examination, and investigation by the system administrators without prior notice or the specific consent of the user. By signing the user agreement form, each authorized user acknowledges the possibility of such Professional employees overseeing student instructional use of the District's computer network or access to the Internet shall be vigilant in determining that students are using the District's system only in compliance with this policy, to enhance student safety and security, particularly when students are using electronic mail, school sanctioned chat rooms authorized under this policy, and other forms of direct electronic communications.

SUSPENDING OR REVOKING PRIVILEGES

Access to the network, the Internet, or both may be suspended or revoked and user IDs deleted if a student or employee is determined to have failed to comply with the standards set by the technology department or violated this policy or the user agreement each user signs as a condition for obtaining access to the District's network and/or the Internet.

Any user identified as a security risk or who has a history of violations with other computer systems shall be denied access to the network. A user whose access has been suspended or revoked may request a conference with the principal and technology director to discuss the basis for that action and have an opportunity to

respond. A decision by the technology director to suspend or revoke system privileges may be appealed to the Superintendent or the Board. System privileges are revoked during any appeal.

ACCEPTABLE USE

Any use described below is deemed “acceptable” and consistent with the user agreement and this policy. The final decision regarding whether any given use of the network or Internet is acceptable lies with the Superintendent or designee, in consultation with the technology director. Acceptable use:

1. Supports instructional purposes and goals.
2. Furthers the District's educational and administrative purposes, goals, and objectives.
3. Furthers research related to education and instruction.
4. Does not violate the Student Code of Conduct or employee standards of conduct.
5. Is consistent with network rules established by the Technology Director.

UNACCEPTABLE USE

Any of the following uses is deemed “unacceptable” and a violation of the user agreement and this policy. The final decision regarding whether any given use of the network or Internet is unacceptable lies with the Superintendent or designee, in consultation with the Technology Director. Unacceptable uses include:

UNACCEPTABLE USAGE AND SYSTEM CONDUCT

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.
3. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.
4. System users must purge electronic mail and data in accordance with established retention guidelines.

5. System users may not redistribute copyrighted programs or data without the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.
6. Real-time discussions, such as in a chat room and instant messaging may only be used for academic purposes under the direct supervision of a teacher. Prior principal approval must be obtained.
7. Students may not distribute personal information about themselves or others by means of the electronic communication system.
8. System users may not send or post messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, illegal, or violent.
9. System users may not purposefully access or redistribute materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, illegal, or violent.
10. System users may not waste District resources related to the electronic communications system
11. System users may not gain unauthorized access to resources or information that is currently blocked by Cameron ISD filtering. This includes the use of proxy servers and other hacking software that defeats installed filtering.
12. All system users are prohibited from playing any type of computer or network game, downloading music, or accessing streaming media not directly related to an approved Cameron ISD curriculum.
13. A system user must receive permission from the Principal or Director of Technology before sending any mass emails to all employees. This will help conserve disk space on the email server.
14. Vandalism and mischief are prohibited. Vandalism includes any attempt to harm or destroy another user's data on the network or streaming media not directly related to an approved CISD curriculum.

VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or data or data of another user of the District's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences.

FORGERY PROHIBITED

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited. The person's user I.D. and/or password are for the exclusive use of the person to whom it has been assigned. The use of another person's user ID and/or password is prohibited.

INFORMATION SUPPLIED BY A THIRD PARTY

System users and parents of students with access to the District's system should be aware that 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.

A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See DH]

DEVELOPMENT OF WEB PAGES

The following Standards will apply to all web sites published in the name of Cameron Independent School District on the World Wide Web or a district Intranet:

Any web pages that are created and maintained in the name of any part of Cameron Independent School District must follow all policy regulations of the school board and district even if the web pages are maintained on a server not owned and operated by Cameron ISD.

1. Web pages for educational purposes will be housed on the Instructional Technology web server. Any department or campus that houses its own server for the purpose of web publishing is responsible for upkeep and maintenance of the web server. All school district policies and regulations including those regarding the Internet must be followed.

2. To access the Instructional Technology web server, an FTP account will be

DATE ADOPTED: August 13, 2007

established in the name of a school district employee. Only this employee will have access privileges.

2. The campus or department supervisor must authorize the creation of any web site. This supervisor must approve the web site and is responsible to ensure that the web site meets all district policies and regulations. If the web site is to be connected to the official district web site, then the Director of Technology must also approve the web site.
3. The campus or department supervisor is responsible for continuous review of the web site to ensure the site meets district policies and regulations including those regarding the Internet.
4. The campus or department is responsible for maintenance and upkeep of the web site.
5. Any links connected to a district approved web site must meet district policy and regulations.
6. All copyright laws must be followed. One should assume that use of anything found on the Internet or the World Wide Web is restricted unless the author gives notice that it is not.
7. Students or employees must obtain a release form to electronically display original work and/or personal images.
8. A release form must be obtained from a parent or guardian before allowing a photograph of a student or any other personally identifiable information to be posted on an Internet page under the District's control.
9. The District will not host or endorse any student's personal web site. If a student creates a website for educational purposes then the district guidelines apply.
10. The district may restrict the size of a web site because of server space.

EMERGING TECHNOLOGIES

New and emerging technologies such as communication devices and software are permitted when used for academic purposes. All new and emerging technologies must have prior approval from the Cameron ISD Technology Director and campus principal. All existing Cameron ISD policies apply.

TERMINATION/REVOCAION OF SYSTEM USER ACCOUNT

The District may suspend or revoke a system user's access to the District's system upon violation of District policy and/or administrative regulations regarding acceptable use.

Cameron ISD
166901

Termination of a user access will be effective on the date the principal or District coordinator receives notice of student/staff withdrawal or resignation or of revocation of system privileges.

DISCLAIMER

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied. The District does not warrant that the functions or services performed by, or that the information or software contained on, the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, 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 the providers and not the District.

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