Employee Guidelines for Acceptable Use of Technology Resources

These guidelines are provided so that employees are aware of the responsibilities they accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, removable media, digitized information, communication technologies, and Internet access. In general, this requires efficient, ethical, and legal utilization of all technology resources.

1. Expectations

a. Use of computers, other technical hardware, computer networks, and software is only allowed when granted permission by the employee's supervisor.

b. All users are expected to follow existing copyright laws. Copyright guidelines are available on the District's web site.

c. Although the District has an Internet safety plan in place, employees are expected to notify their campus or district administrator whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

d. Employees who identify or know about a security problem are expected to convey the details to their campus or district administrator without discussing it with others.

e. Employees are responsible for securing technology devices when not in use and for returning them in good working condition.

f. Employees have a right to participate in social networking sites, blogs, forums, wikis, etc., or other Internet activities for their private use; however, employees should not post anything (through written messages, images, videos, or otherwise that would violate student confidentiality rights, and/or District Board policies and procedures including but not limited to the Code of Ethics and Standard Practices for Texas Educators, and/or that would negatively impact the perception of the employee's ability to be effective in their employment capacity. Postings that are considered inappropriate or otherwise are violations of District Board policies and procedures, including but not limited to the Acceptable Use Procedures, may be addressed by the District and could lead to disciplinary action up to and including termination.

2. Unacceptable conduct includes but is not limited to the following:

a. Using the network for illegal activities, such as copyright or contract violations, or downloading inappropriate materials, viruses, and/or software, including but not limited to hacking and host file sharing software.

b. Using the network for financial or commercial gain, advertising, or political activities.

c. Accessing or exploring online content that does not support the curriculum and/or is inappropriate for school assignments, including but not limited to pornographic sites.

d. Vandalizing, tampering, or accessing without permission, equipment, programs, files, software, system performance or other technology. Use or possession of hacking software is strictly prohibited.

e. Causing congestion on the network or interfering with the work of others, e.g., chain letters, jokes, or pictures to lists or individuals.

f. Unauthorized or non-curricular use of online video, music, or streaming content.

g. Gaining unauthorized access anywhere on the network.

h. Invading the privacy of other individuals.

i. Using another user's account, password, or allowing another user access to your account, password.

j. Coaching, helping, joining, or acquiescing in any unauthorized activity on the network.

k. Posting anonymous, unlawful, or inappropriate messages or information on a district-owned system.

l. Engaging in sexual harassment or using any language of a sexual or otherwise objectionable nature (e.g., racist, terroristic, abusive, threatening, demeaning, slanderous) in public or private messages.

m. Falsifying permission and/or authorization of identification documents.

n. Obtaining copies of or modifying files, data, or passwords belonging to other users on the network without authorization.

o. Knowingly placing a computer virus on a computer or network.

p. Transmission of any material that is in violation of any federal or state law. This includes, but is not limited to, student or other confidential information, copyrighted material, threatening or obscene material, and computer viruses.

3. Acceptable Use Guidelines

a. General Guidelines:

(1) Employees are responsible for the ethical and educational use of technology in the District and when a district-owned device is used out of District.

(2) Employees will have access to available forms of electronic media and communication that is in support of education and research, and in support of the educational goals and objectives of the District.

(3) All technology policies and restrictions must be followed.

(4) Access to the District's computer online services is a privilege and not a right. Each employee will be required to sign and adhere to the Acceptable Use Procedures Agreement.

(5) When placing, removing, or restricting access to data or online services, school officials shall apply the same criteria of educational suitability used for other education resources.

b. Network Etiquette

(1) Be polite.

(2) Use appropriate language.

(3) Do not reveal personal data (i.e. home address, phone number, or phone numbers of other people).

(4) Remember that the other users of technology are human beings whose culture, language, and humor have different points of reference from your own.

(5) Users should be discrete when forwarding e-mail and it should only be done on a need-to-know basis.

c. E-Mail

(1) E-mail may be used for educational or administrative purposes only.

(2) E-mail transmissions, stored data, transmitted data, or any other use of district-owned technology by employees or any other user is subject to being monitored at any time by designated staff to ensure appropriate use.

(3) All e-mail and all contents are property of the District.

d. Consequences

The employee, in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use. Noncompliance with the guidelines published here, in the Employee Code of Conduct, and in Board policy may result in suspension or termination of technology privileges and disciplinary action. Violations of applicable state and federal law, including the Texas Penal Code, Computer Crimes, Chapter 33 may result in criminal prosecution, as well as disciplinary action by the District. The District cooperates fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. In addition, contents of e-mail and network communications using District equipment and network access is governed by the Texas Public Information Act, and therefore may be subject to public disclosure as required by law. Any attempt to alter data, the configuration of a computer, or the files of another user, without the consent of the campus or district administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with Board policy.

Employee Name (print)

_____

School/Location

_____

I have read the Employee Acceptable Use Guidelines for Colmesneil ISD. I agree to follow the rules contained in these guidelines. I further understand that electronic mail transmissions and other use of the electronic communications systems, including the Internet, are not private and may be monitored at any time by the District staff to ensure appropriate use, as defined by the Acceptable Use Guidelines. I understand that violations can result in disciplinary action, up to and including termination of employment.

Employee Signature:

_____