

# Student Guidelines for Acceptable Use of Technology Resources

These guidelines are provided so that students and parents are aware of the responsibilities students 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. Student use of computers, other technology hardware, software, and computer networks, including the Internet, is only allowed when supervised or granted permission by a teacher or campus/district administrator.

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, students are expected to notify a staff member whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

d. Students who identify or know about a security problem are expected to convey the details to their teacher or campus/district administrator without discussing it with other students.

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

a. Using the network for illegal activities, such as copyright, license, 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 to access 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, stalking, or 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 confidential information, copyrighted material, threatening or obscene material, and computer viruses.

### **3. Acceptable Use Guidelines**

#### **a. General Guidelines**

(1) Students 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) Students 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 student will be required to sign and adhere to the Acceptable Use Guidelines 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.

(6) Any parent wishing to restrict their children's access to any District computer online services will need to provide this restriction request in writing. Parents will assume responsibility for imposing restrictions only on their own children.

#### **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. Students are provided a Google e-mail account.

(2) E-mail transmissions, stored data, transmitted data, or any other use of district-owned technology by students 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.

### **4. Consequences**

The student 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 may result in suspension or termination of technology privileges and disciplinary action. Use or possession of hacking software is strictly prohibited and

violators will be subject to consequences in the Student Handbook / Student Code of Conduct. 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 are 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 individual, campus or district administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the Student Handbook / Student Code of Conduct.

## **5. Web 2.0 and Social Media Tools**

### **a. Approved for Classroom Use**

(1) Colmesneil ISD students, under the supervision and guidance of their teachers will use Web 2.0 and social media tools commonly used in K- 12 education today as part of instruction in their classrooms. Such tools may include but are not limited to: Google Apps, Project Share, Scholastic, JSTOR, BrainPop, Study Island, and others.

(2) Students use these tools to meet the communication, collaboration, creation, research, and information fluency skills required by the Texas Essential Knowledge and Skills (TEKS). Tools such as these are hosted on the Internet making some of the students' work and/or other information relating to students visible to parents/guardians/relatives, and in some circumstances, other Internet users around the world.

### **b. Safety**

(1) When using Web 2.0 and social media tools, the following safeguards are in place to protect and assure the safety of students. Please be aware that in rare instances:

- Individual or identifiable profiles (which include personally identifiable information of students such as first and last name, campus, etc.) may be used that are open to the public.

- Public viewing and commenting might occur on district-approved sites.
- Classroom lessons or projects may require publicly identifiable student information (first and last name, campus, etc.) to be made available on the Internet.

(2) Use of these tools must be in accordance with the Colmesneil ISD's Policies and Procedures including but not limited to these Acceptable Use Procedures.

Student Name (print)

---

School/Location

---

I have read the Student 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.

Student Signature:

---