

EMPLOYEE GUIDELINES FOR ACCEPTABLE USE OF TECHNOLOGY RESOURCES (III-36.4)

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 posted and/or available in the media center of each campus as well as posted 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 (as stated in Board policy DH (EXHIBIT)), 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.
- g. Employees are responsible for conserving energy as appropriate by turning off electronic devices daily.

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 ID card or allowing another user access to your account, password, or ID.

- 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. Using personal computing devices on the district network, except district-approved devices.
 - q. 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 districtowned 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 Klein 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: _____

PROCEDURE FOR PROFESSIONAL AND PERSONAL USE OF SOCIAL AND OTHER ELECTRONIC MEDIA – DISTRICT OR NON-DISTRICT OWNED (III-36.5)

This directive applies to Web 2.0 tools and provides instruction on the proper use of these tools. The tools are included but not limited to the following whether or not used on equipment or software owned by the District:

- Text messaging
- Instant messaging
- Electronic Mail (e-mail)
- Web logs (blogs)
- Wikis
- Electronic forums (e.g., chat rooms)
- Video Sharing Web sites (e.g., YouTube)
- Editorial comments posted on the Internet
- Social network sites (e.g., FaceBook, MySpace, Twitter, and LinkedIn)

Technology-based materials, activities, and communication tools shall be appropriate for and within the range of the knowledge, understanding, age, and maturity of the students with whom they are used.

Use of Electronic Media for Klein ISD Purposes

The District believes that the use of electronic media in the classroom and extracurricular setting can be beneficial to students and parents in the educational process and in the efficient

communication of information. However, any District employee or activity sponsor wishing to use electronic media with or for communication with students must comply with these guidelines.

Employees and activity sponsors must only use District owned/purchased, or supported products. Currently, these products include, but are not limited to, ParentLink, Gaggle, Project Share, Google Apps, and Klein Private Label Wiki. The employee or activity sponsor must maintain and is responsible for all communication within the blog or social network account and cannot turn the responsibility over to a student or parent. Employees and activity sponsors may not use other social networking sites for these purposes (private blogs or chat rooms, FaceBook, Twitter, MySpace, YouTube, etc).

In order for District employees and activity sponsors to utilize district-approved social networking sites for instructional, administrative, or other work-related communication purposes, they shall comply with the following:

1. They shall request, in writing, prior permission from the building principal.
2. If permission is granted, staff members will set up the site following any District guidelines developed by the building principal and Superintendent's designee in accordance with District policies and procedures.
3. Have written parent permission from each student invited to the site on file in accordance with the record retention policies. The permission form can be accessed on Klein share, titled *Klein ISD Student Social Media Participation Form*.
4. Allow the building principal or his/her designee to have access to the site at all times.
5. Once the site/resource has been created, the staff member is responsible for the following:
 - Monitoring and managing the site to promote safe and acceptable use;
 - Keeping the site private and accessible only to students, parents, and campus administrators;
 - Observing confidentiality restrictions concerning release of student information under state and federal law;
 - Not posting student names, photographs or videos in which students appear on personal online social media. The proper forms must be completed for each student in order to post this type of information.
 - Confidentiality of student records;
 - Confidentiality of health or personnel information concerning colleges, unless disclosure serves lawful professional purposes or is required by law;
 - Confidentiality of District records, including educator evaluations and private e-mail addresses, phone numbers, etc.;
 - Prohibition against harming others by knowingly making false statements about a colleague or the school system.
6. Parents and administrators will be included in all site/resource communication to ensure guidelines are being followed.
7. Parents have the ability to opt out of the request for social media communication for their child without any penalty to his/her child.
8. Communication with students, using these District-approved forms of electronic media, shall be done only during the hours of 6:00 a.m. through 9:00 p.m.

Text Messaging with Students

Communication with students through the use of text messaging is permitted only by staff members who have extracurricular responsibilities and the students participating in the extracurricular activity over which the employee is responsible.

All communication must comply with the following rules:

- Prior to the first communication in a school year, the parent must grant written permission for each staff member the parent will allow to communicate via text message with his/her child. A parent must agree that he/she can be copied on all text messages;
- Be professional and appropriate;
- Be limited to matter within the scope of the employee's professional responsibilities;
- Include the parent in all communication to the students except in the case of a health or safety emergency (change in practice times is not a health or safety emergency);
- Be limited to the hours of 6:00 a.m. – 9:00 p.m. unless addressing a matter of immediate concern;
- These rules do not apply to the extent an employee has a social or family relationship with a student.
- All consent forms must be kept at the campus for future reference.

Personal Use of Electronic Media:

Employees are held to the same professional standards in their public use of electronic media as they are for any other public conduct. Each employee is responsible for all the content on any social network site the employee maintains (whether or not posted by the employee) and for choosing privacy settings appropriate to the content.

Employees who maintain their own personal electronic media or social networking sites for their private use will not share their personal networking sites with students or include students as members, friends, or links or other associations on the site except as may be specifically allowed by Board Policy or these guidelines.

If an employee posts messages or picture on social media sites or other web resources which diminish the employee's professionalism or discredit the employee's capacity to maintain the respect of students and parents, it will impair the employee's ability to effectively perform their job. This type of material includes, but is not limited to, text or pictures involving hate speech, nudity, obscenity, vulgarity, and conduct illegal for minor or sexually explicit content. **Such conduct may be grounds for termination or other disciplinary action.**

An employee who uses electronic media for personal purposes shall comply with the following:

- The employee shall limit use of personal electronic communication devices to send or receive calls, text messages, picture messages, or video messages to their break time, meal time, or before or after scheduled work hours, except for an emergency or when use is authorized by a supervisor for the purpose of conducting District business;
- The employee may not create or update a personal social networking page(s) or make posts or blog on such personal pages using the District's computers, network, or equipment;
- The employee shall not use the District's or any campus logo without the written consent of the employee's supervisor;
- The employee may not post any information regarding any Klein ISD student or employee which would violate District, state, or local law.