Technology Acceptable Use Policy

Technology Resources

Reference Policy CQ (Legal) (Local)

The district's technology resources, including its networks, computer systems, e-mail accounts, devices connected to its networks, and all district-owned devices used on or off school property are primarily for administrative and instructional purposes. Limited personal use is permitted if the use:

- Imposes no tangible cost to the district
- Does not unduly burden the district's technology resources
- Has no adverse effect on job performance or on a student's academic performance

Electronic mail transmissions and other use of technology resources are not confidential and can be monitored at any time to ensure appropriate use.

Employees are required to abide by the provisions of the district's acceptable use agreement and administrative procedures. Failure to do so can result in suspension or termination of privileges and may lead to disciplinary and legal action. Employees with questions about computer use and data management can contact the Executive Director of Technology.

Personal Use of Electronic Communications

Reference Policies CQ (Legal) (Local) DH (Local)

Electronic communications includes all forms of social media, such as text messaging, instant messaging, electronic mail (email), Web logs (blogs), wikis, electronic forums (chat rooms), video sharing websites (e.g., YouTube), editorial comments posted on the Internet and social network sites (e.g., Facebook, Twitter, LinkedIn, Instagram). Electronic communications also include all forms of telecommunication such as landlines, cell phones, and web-based applications.

As role models for the district's students, employees are responsible for their public conduct even when they are not acting as district employees. Employees will be held to the same professional standards in their public use of electronic communications as they are for any other public conduct. If an employee's use of electronic communications interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment. If an employee wishes to use a social network site or similar media for personal purposes, the employee is responsible for the content on the employee's page, including content added by the employee, the employee's friends, or members of the public who can access the employee's page, and for web links on the employee's page. The employee is also responsible for maintaining privacy settings appropriate to the content.

An employee who uses electronic communications for personal purposes shall observe the following:

- The employee may not set up or update the employee's personal social network page(s) using the district's computers, network, or equipment.
- The employee shall limit use of personal electronic communication devices to send or receive calls, text messages, pictures, and videos to breaks, meal times, and before and after scheduled work hours, unless there is an emergency or the use is authorized by a supervisor to conduct district business.
- The employee shall not use the district's logo or other copyrighted material of the district without express, written consent.
- An employee may not share or post, in any format, information, videos, or pictures obtained while on duty or on district business unless the employee first obtains written approval from the employee's immediate supervisor. Employees should be cognizant that they have access to information and images that, if transmitted to the public, could violate privacy concerns.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the *Texas Educators' Code of Ethics*, even when communicating regarding personal and private matters, regardless of whether the employee is using private or public equipment, on or off campus. These restrictions include:
    - Confidentiality of student records. Reference Policy FL (Legal) (Local)
    - Confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law. Reference Policy DH (Exhibit)
    - Confidentiality of district records, including educator evaluations and private email address. Reference Policy GBA (Legal)
    - Copyright law. Reference Policy CY (Legal) (Local)
    - Prohibition against harming others by knowingly making false statements about a colleague or the school system. Reference Policy DH (Exhibit)

See *Electronic Communications between Employees and Students*, below, for regulation on employee communication with students through electronic media.

Electronic Communications between Employees and Students

Reference policy DH (Local)

A certified or licensed employee, or any other employee designated in writing by the superintendent or a campus principal, may use electronic communications with students who are currently enrolled in the district. The employee must comply with the provisions outlined below. Electronic communications between all other employees and students who are enrolled in the district are prohibited. Employees are not required to provide students with their personal phone number or e-mail address.

An employee is not subject to the provisions regarding electronic communications with a student to the extent the employee has a social or family relationship with a student. For example, an employee may have a relationship with a niece or nephew, a student who is the child of an adult friend, a student who is a friend of the employee's child, or a member or participant in the same civic, social, recreational, or religious organization. An employee who claims an exception based on a social relationship shall provide written consent from the student's parent. The written consent shall include an acknowledgement by the parent that:

- The employee has provided the parent with a copy of this protocol
- The employee and the student have a social relationship outside of school;
- The parent understands that the employee's communications with the student are excepted from district regulation; and
- The parent is solely responsible for monitoring electronic communications between the employee and the student.

The following definitions apply for the use of electronic media with students:

Electronic communications means any communication facilitated by the use of any electronic device, including a telephone, cellular telephone, computer, computer network, personal data assistant, or pager. The term includes e-mail, text messages, instant messages, and any communication made through an Internet website, including a social media website or a social networking website.

- *Communicate* means to convey information and includes a one-way communication as well as a dialogue between two or more people. A public communication by an employee that is not targeted at students (e.g., a posting on the employee's personal social network page or a blog) is not a communication: however, the employee may be subject to district regulations on personal electronic communications. See *Personal Use of Electronic Communications*, above. Unsolicited contact from a student through electronic means is not a communication.

- *Certified or licensed employee* means a person employed in a position required SBEC certification or a professional license, and whose job duties may require the employee to communicate electronically with students. The term includes classroom teachers, counselors, principals, librarians, paraprofessionals, nurses, educational diagnosticians, licensed therapists, and athletic trainers.

An employee who communicates electronically with students shall observe the following:

- The employee is prohibited from knowingly communicating with students using any form of electronic communications, including mobile and web applications, that are not provided or accessible by the district unless a specific exception is noted below.
- Only a teacher, trainer, or other employee who has an extracurricular duty may use text messaging, and then only to communicate with students who participate in the extracurricular activity over which the employee has responsibility. An employee who communicates with a student using text messaging shall comply with the following protocol:

- The employee shall include at least one of the student's parents or guardians as a recipient on each text message to the student so that the student and parent receive the same message;
- The employee shall include his or her immediate supervisor as a recipient on each text message to the student so that the student and supervisor receive the same message; or
- For each text message addressed to one or more students, the employee shall send a copy of the text message to employee's district e-mail address.

- The employee shall limit communications to matters within the scope of the employee's professional responsibilities (e.g., for classroom teachers, matters relating to class work, homework, and tests; for an employee with an extracurricular duty, matters relating to the extracurricular activity.)
- The employee is prohibited from knowingly communicating with students through a personal social network page; the employee must create a separate social network page ("professional page") for the purpose of communicating with students. The employee must enable administration and parents to access the employee's professional page.
- The employee shall not communicate directly with any student between the hours of 10 pm and 6 am. An employee may, however, make public posts to a social network site, blog, or similar application at any time.
- The employee does not have a right to privacy with respect to communications with students and parents.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Texas Educators' Code of Ethics including:
    - Compliance with the *Public Information Act and the Family Educational Rights and Privacy Act* (FERPA), including retention and confidentiality of student records. [See Policies CPC and FL]
    - Copyright law. [See Policy CY]
    - Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student. [See Policy DH]

- Upon request from administration, an employee will provide the phone number(s), social network site(s), or other information regarding the method(s) of electronic media the employee uses to communicate with one or more currently-enrolled students.
- Upon written request from a parent or student, the employee shall discontinue communicating with the student through email, text messaging, instant messaging, or any other form of one-to-one communication.
- An employee may request an exception from one or more of the limitations above by submitting a written request to his or her immediate supervisor.
- An employee shall notify his or her supervisor in writing within one business day if a student engages in an improper electronic communications with the employees. The employee should describe the form and content of the electronic communication.

Additional Guidelines

Consequences of Improper Use

Violation of WISD's policies and procedures concerning the use of computers and networks will result in the same disciplinary actions that would result from similar violations in other areas of WISD. Improper or unethical use may result in disciplinary actions consistent with the existing Student Discipline Policy and, if appropriate, the Texas Penal Code, Computers Crimes, Chapter 33, or other state and federal laws. This may also require restitution for costs associated with system restoration, hardware, or software costs. The district will cooperate fully with local, state, or federal officials in any invitation concerning or relating to misuse of the District's computer systems and networks.

Illegal Activity

Transmission (that is, uploading or downloading) of any material in violation of any national, state or local regulation is prohibited. This includes, but is not limited to:

- Copyrighted material
- Abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, illegal material
- Material protected by trade secret
- Commercial activities such as conducting private business on the Internet
- Transmission for advertisement or political use

Consent Requirements

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the copyright owner, or an individual the owner specifically authorizes, may upload or redistribute copyrighted material to the system.

No original work created by a District student or employee will be posted on a web page under the District's control unless the District has received written consent from the student (and the student's parent if the student is a minor) or employee who created the work.

No personally identifiable information about a District student will be posted on a web page under the District's control unless the District has received written consent from the student's parent. The *Family Educational Rights and Privacy Act* and District policy may make an exception for "directory information" as allowed.

Security

The security of any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the network, you are required to notify a system administrator or school personnel. Do not demonstrate the problem to other users. Do not use another individual's account.

Etiquette

Users are expected to abide by the generally accepted rules of communications etiquette. These include, but are not limited to, the following:

- Be polite. Do not send or post abusive messages.
- Use appropriate language. Do not swear, use vulgarities, sexually suggestive language, or any other inappropriate language.
- Exercise caution when using WISD communications tools to email or post your opinions. Recipients or other readers may assume that your opinion represents the views of the District or school, whether or not that was your intention.
- Do not reveal your personal address or phone number or the address or phone number of students or colleagues.
- Check your email at least once a day. Reply to email from parents or other public members who have legitimate business requests within 24 hours whenever possible.
- Share your WISD email address with interested parents and community members who request to communicate with you in this fashion.
- Do not send messages to an entire staff when only a small group of people actually needs to receive the message. In accordance with established procedures, using email for commercial enterprises is prohibited.
- Do not forward messages that have no educational or professional value (e.g., chain letters.)

Email

The following guidelines will apply to all users of the District's electronic communications systems:

- Users will be issued only one district email account.
- Communications may not be encrypted so as to avoid security review by system administrators.

- Attachments to email messages should include only data files. At no time should program files (e.g. .exe files) be attached due to risk of licensing violations and transmission of viruses.
- Requests for personal information on students or staff members should not be honored via email. This relates particularly to any requests for student grades, discipline, attendance or related information. In addition, security information such as usernames or passwords should not be sent via email for any reason.

Responsible Network Use

The individual in whose name a system account is issued will be responsible at all times for its proper use and to abide by the generally accepted guidelines for responsible network use. System users *may not*:

- Utilize the District network for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.

- Disable, or attempt to disable, a filtering device on the District's electronic communications system.

- Establish peer-to-peer networking.

- Create unauthorized wireless networks, including wireless access points, wireless routers and open networks on personal devices.

- Use any software or proxy service to obscure the student's IP address or sites that the student visits.

- Use another person's system account without written permission from the campus administrator.

- Gain unauthorized access to resources or information.

- Place the District network and equipment at risk of viruses and other harmful codes by opening email messages from unknown senders, loading data from unprotected computers, etc.

Equipment Guidelines

All technology equipment should be shut down each evening.

District personnel are responsible for District equipment if taken off school property. Traveling personnel must secure equipment every night to not be liable.

As personnel transfer to other locations within the District, the equipment they utilized at

their originating campus must remain on that campus. To maintain accurate inventories and comply with state and federal funding guidelines, staff members are not allowed to transfer computers and other technology equipment to their new campus.

Vandalism

Any malicious attempt to harm or destroy District equipment or data or the data of another user of the District's system or of 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. [See DH, FN series, and the FO series]

Employees with questions about computer use and data management may contact Deborah Menefee, Executive Director of Technology at 936-856-1212 or dmenefee@willisisd.org.