Wharton ISD – Staff Acceptable Use Policy 2022-2023

Technology Resources

All network and computer equipment is the property of Wharton ISD. The District's technology resources, including its network, computer systems, email accounts, devices connected to its network, and all district-owned devices used on or off school property, are primarily for administrative and instructional purposes. Electronic transmissions and other use of the technology resources, including Google Drive, are not confidential and can be monitored at any time to ensure appropriate use.

Wharton ISD's system will be used only for administrative and educational purposes consistent with the District's mission and goals. The District is authorized to monitor or examine all system activities, including electronic mail and internet use, as deemed appropriate to ensure proper use of the system.

Employees shall be held to the same professional standards in their public use of electronic media as they are for any other public conduct. If an employee's use of electronic media violates state federal law or District policy, or 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. (Board Policy DH Local-A, page 1 and 2)

It is the policy of Wharton ISD to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via the internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

It shall be the responsibility of the Wharton ISD staff to educate, supervise and monitor appropriate usage of the online computer network and access to the internet in accordance with this policy, the Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Online Conduct

1. The individual in whose name a system account is issued will be responsible at all times for its proper use, including securing your password.
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. Use for commercial, income-generating or "for-profit" activities, product advertisement, or political lobbying is prohibited by users.
4. Sending unsolicited junk mail or chain letters is prohibited.
5. System users may not use another person's system account without written permission from the District coordinator, as appropriate.
6. Employees may not install any software, including but not limited to commercial software, shareware, freeware, original software and/or utilities on school computers or networks.
7. **Employees may not install or run executable applications and software from the Internet, including the use of proxy servers to bypass the WISD "Content Filter" to run. Use of any proxy server to bypass the WISD Content Filter (as required by the Children's Internet Protection Act- CIPA) is considered a severe violation. Only the**

Director of Technology may authorize the installation of technology purchases and, in most cases, only the Technology Department personnel are permitted to install such technology purchases. Bypassing district filters and security via proxy servers, VPN access or other means will not be tolerated and considered a violation of the WISD Acceptable Use Policy.

8. System users may redistribute copyrighted programs or data only with 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 in accordance with applicable copyright laws, District policy, and administrative regulations.
9. Any user who knowingly brings prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.
10. Personal laptops are not supported on our network.

Digital Citizenship

System users are expected to observe the following etiquette:

1. Be polite
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
3. Pretending to be someone else when sending/receiving messages is considered inappropriate.
4. Transmitting obscene messages or pictures is prohibited.
5. Revealing personal addresses or phone numbers of the user or others is prohibited.

Vandalism Prohibited

Any malicious attempt to harm or destroy District equipment or materials, 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 may be viewed as violations of District policy and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses. Vandalism will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, hardware, or software costs.

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 to send/receive electronic mail is prohibited.

Revocation of 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. Termination of an employee's account or of a student's access will be effective on the date the principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

Personal Use of Electronic Communications

Electronic media includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), Web logs (blogs), electronic forums (chat rooms), video-sharing websites, editorial comments posted on the Internet, and social network sites. Electronic media also includes all forms of telecommunication, such as landlines, cell phones, and Web-based applications. (Board Policy DH Local-A, page 1)

Acceptable Use. The purpose of the WISD network is to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work. Access to the District's technology resources, including the Internet, shall be made available to employees exclusively for instructional and administrative purposes and in accordance with administrative regulations.

Employees who are authorized to use the system are required to abide by the provisions of the acceptable use policy and administrative procedures. Failure to do so can result in suspension of access or termination of privileges and may lead to disciplinary action.

All District employees authorized to access sensitive or confidential student or employee information are expected to maintain the security of the storage, access, transmission and transportation of such information. Any breach of the security of such information may lead to disciplinary action.

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/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 form at, 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 58 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; [See Policy FL]
- Confidentiality of health or personal information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law; [See Policy DH (EXHIBIT)]
- Confidentiality of District records, including educator evaluations and private email addresses; [See Policy GBA] copyright law [See Policy CY]

- Prohibition against harming others by knowingly making false statements about a colleague or the school system [See Policy DH (EXHIBIT)]

Use of Electronic Media with Students

A certified or licensed employee, or any other employee designated in writing by the superintendent or a campus principal, may communicate through electronic media with students who are currently enrolled in the district. The employee must comply with the provisions outlined below.

Employees are not required to provide students with their personal phone numbers or email address.

Texting should not occur between 10:00 p.m. and 7:00 a.m. unless extenuating circumstances exist and it is imperative to communicate the message. All other employees are prohibited from using electronic media to communicate directly with students who are currently enrolled in the District.

An employee is not subject to these provisions 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 accepted 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 media* includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), 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 media* also includes all forms of telecommunication such as landlines, cell phones, and web-based applications.
- *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 Media*. Unsolicited contact from a student through electronic means is not a *communication*.
- *Certified or licensed employee* means a person employed in a position requiring 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 uses electronic media to communicate with students shall observe the following:

1. The employee may use any form of electronic media **except** text messaging. Only a teacher, trainer, or other employees who has an extracurricular activity 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 receives 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 receives the same message; or copy of the text message to the employee's district e-mail address.

2. 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 test; for an employee with an extracurricular duty, matters relating to the extracurricular activity).

Professional Social Network Site
The employee is prohibited from knowingly communicating with students through a personal social network page;

- The employee must request a separate social network page ("professional page") for the purpose of communicating with students through the WISD Director of Technology.
- The employee must enable administration and parents to access the employee's professional page.
- The employee does not have a right to privacy with respect to communications with students and parents.

.

Disclaimer
The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that 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 misuse of the District's electronic communications system.

Return of Technology Resources and Records
Upon leaving employment, or upon request from the Superintendent, you must return any District-owned equipment or resources in your possession. You must also return any records, written or electronic, to the District for records retention if you have reason to believe you are

retaining the sole copy of a record subject to records retention requirements. You must destroy (delete or shred) any other confidential records remaining in your possession.

Notice: The Technology Department reserves the right to remote in on any district device to perform maintenance at any time. If the Technology Department deems a device is unsafe due to a virus, they will come take the device immediately to maintain the integrity of our network.

Wharton Independent School District
AUP Signature Page for 2022-2023 School Year:

I understand that my use of the District's technology resources is not private and that the District will monitor my activity.

I have read the District's technology resources policy, associated administrative regulations, and this is your agreement and agree to abide by the provisions of Wharton ISD. In consideration for the privilege of using the District's technology resources, I hereby release the District, its operators, and any institution with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, these resources, including, without limitation, the type of damages identified in the District's policy and administrative regulations.

I understand that this user agreement must be renewed each school year. If you have any questions concerning this document, please contact Heath Roddy, WISD Director of Technology, at 979-488-2595.

Signature: _____

Campus: _____

Date: _____