Operations Handbook

Technology

Technology Department

Our Mission

The WISD ISD Technology Department strives to ensure that our students are provided with the most modern and advanced technical resources to maximize the learning environment.

By providing leadership, network infrastructure, instructional support, and professional development, the Technology Department will empower students, educators, staff, and the community to utilize current and emerging technologies as tools for life-long learning.

Technology Staff

Heath Roddy
Director of Technology

Stacie Boudrie
Assistant Director of Technology & Integration Specialist

Doris Dornak
Tech Specialist

Michael Munoz
Tech Specialist

Technology

Heath Roddy, Director of Technology, 979-488-2595

Support / Infrastructure Services

Heath Roddy, Technology Director

The Support Services Team is responsible for providing prompt, courteous, and quality customer service to the students, staff, and administrators of Wharton ISD. This team responds to technical work orders and provides 1st and 2nd level maintenance and support for all end-user computer and instructional tools, manages the IT procurement and asset management process, coordinates the selection and rollout of new computer systems and ensures all systems are up-to-date with the latest approved images and software packages.

Integration Services

The Integration Services Team is responsible for providing technology integration, training, and support to all staff members. This team works closely with the Learner Services Division to enhance the integration and support of instructional tools into daily curriculum and instruction. They provide training and assistance to campus technicians in supporting applications, video delivery, mobile, and end-user devices.

Stacie Boudrie, Assistant Technology Director & Integration Specialist

Tech Support

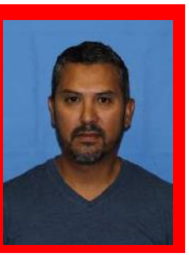
Doris Dornak

Tech Specialist

- District Webpage
- District Xerox Printers
- Troubleshooting Computers
- Chromebook repair
- Remote assist
- Tech Tickets
- Inventory

Doris Dornak

Tech Specialist



- Whispercast/Kindle repair
- Printers
- Troubleshooting Computers
- Chromebook repair
- Remote assist
- Tech Tickets
- iPad setup

Technology

Heath Roddy, Director of Technology, 979-488-2595

Technology Policies and Strategies

Scope

This policy applies to anyone who uses Wharton Independent School District technology resources. Technology resources include all District owned, licensed, or managed hardware and software as well as the use of the District network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Definitions

The District's computer systems and networks include but are not limited to the following:

- Computer hardware and peripherals
- Servers
- Email
- Software including operating system software and application software
- Externally accessed data including the Internet
- Network storage
- District provided Internet access
- District provided public Wi-Fi
- New technologies as they become available

Policy

It is the policy of Wharton ISD to:

- 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;
- prevent unauthorized access and other unlawful online activity;
- prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
- Comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Acceptable Use:

The District's technology resources will be used for learning, teaching, and administrative purposes consistent with the District's mission and goals.

Digital Citizenship

System users are expected to observe the following etiquette:

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

Online Conduct:

- The individual in whose name a system account is issued will be responsible at all times for its proper use, including securing your password.
- The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.
- Use for commercial, income-generating or "for-profit" activities, product advertisement, or political lobbying is prohibited by users.
- Sending unsolicited junk mail or chain letters is prohibited.
- System users may not use another person's system account without written permission from the District coordinator, as appropriate.
- 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.
- 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.
- Any user who knowingly brings prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.

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)

Improper Use Includes:

- Submitting, publishing or displaying any defamatory, cyber bullying, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private;
- Attempting to or physically damaging equipment, materials or data;
- Attempting to or sending anonymous messages of any kind, except as expressly allowed by the District's Elevate system;
- Pretending to be someone else when sending/receiving messages;

Technology

Heath Roddy, Director of Technology, 979-488-2595

- Using District resources for personal and commercial use;
- Using the network to access inappropriate material;
- Knowingly placing a computer virus on a computer or the network;
- Opening email messages from unknown senders, loading data from unprotected computers, and any other risky action that may introduce viruses to the system;
- Accessing of technology resources, files and documents of another user without authorization;
- Attempting to or using proxy servers or otherwise bypassing security to gain access to the Internet or network resources;
- Posting personal information about others without proper authorization;
- Attempting to "hack" into technology resources;
- Storing inappropriate information (i.e. programs,.exe files, non-work related videos);
- Attempts to degrade or disrupt resource performance including but not limited to denial of service attacks;
- Any interference with the work of others, with or without malicious intent;
- Forgery or attempted forgery of electronic messages or data;
- Violation of copyright laws;
- Installing software without proper approval;
- Installing or setting up any device that would alter the network topology including wireless access points, routers, hubs, or switches;
- Modifying desktop/laptop configurations including altering desktop backgrounds, screensavers, power settings or any other pre-configured setting;
- Attempting to gain unauthorized access to 3rd party networks or systems through the use of District resources.

Network Access:

Access to the District's network systems will be governed as follows:

- Users with accounts will be required to maintain password confidentiality by not sharing the password with others. Your username and password should be protected from unauthorized use at all time. Do not post any password information where others can view it and do not send via mail.
- Use passwords that are difficult to guess and make sure not to store passwords in easily accessed locations. Password phrases are easier to remember and more secure (ex: Ilovesummer18!).
- Any system user identified as a security risk or having violated the Technology Acceptable Use Policy may be denied access to the District's system. Other consequences may also be administered.
- You should lock your workstation to secure your computer whenever it is not in use. If you are logged into the network, leaving a computer unlocked and unattended enables anyone to potentially access your grade book, email, and/or other personal or information-sensitive files. Workstations can be locked by pressing "CTRL-ALT-DEL" and selecting the "Lock Workstation" option.

Technology

Heath Roddy, Director of Technology, 979-488-2595

- The individual in whose name a system account is issued will be responsible at all times for its proper use.
- The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District guidelines.

Technology Support

Tech Ticket
Directions for submitting a WISD Tech Ticket - **https://tinyurl.com/ybwczyl4**

All Requests for support need to be documented by inputting a Tech Ticket. Once Tech Ticket is submitted, it will be assigned a repair time. Repairs needed that directly impact students and teacher instruction will take a high priority. Response to help desk calls will be within one working day on the highest priority, two days on normal priority and four days on the lowest priority. This response period does not mean the problems will be solved within this time but that the technician will look at the problem and establish the corrective action. If additional time is required (i.e. ordering of parts), the user will be notified, and a spare piece of equipment will be given if available.

The Technology Department is available for questions regarding application issues or other issues were the users can be guided through the problem. If possible technology staff may utilize software that allows for viewing of the user's desktop or may require the user to log off of his/her workstation. If the Help Desk technician is unable to correct the problem through phone support, the call will be logged, given a priority, and assigned repair time.

Support Numbers:

- Technology Specialist (979) 488-2594 Ext. 1594- Log-in problems, e-mail issues, application support, computer maintenance and repair, IVN Meeting and room issues, media cart requests, printing. (WAN/LAN/wireless issues, classroom software systems, & print service Issues.
- Director of Technology (979) 488-2595 Ext. 1595 - Log-in problems, e-mail issues, application support, computer maintenance and repair, networking issues, . (WAN/LAN/wireless issues, Classroom software systems, & print service Issues, issues concerning purchasing of equipment, software.

Technology Office Hours
Monday through Friday 6:00am – 4:30pm. Support can be provided during evenings and weekends with advance notice and with approval of the Director of Technology.

Contact Person

Director of Technology: All hardware and software repairs, network (cables), WiFi, teacher Google Drive accounts, printers, locked accounts, request for new software, unblocking of educational sites. The

Technology

Heath Roddy, Director of Technology, 979-488-2595

Director of Technology oversees all tech request, tech purchases, tech planning, networking/WIFI and integration needs provided at WISD.

Assistant Director of Technology/Integration Specialist: Direct instruction support with technology integration that includes online web tools (myON, Discovery Education, Imagine Math, etc.), student Google Drive accounts, and implementation of hardware a/o software.

Technology Specialist: The Technology Specialist supports the needs of hardware (computers, laptops, Chromebooks, printers) or software repaired. Please put in a tech ticket for the Technology Specialist to repair your device.

School Website

Wharton ISD website is maintained by the Technology Department. If you would like something posted on district website send your request to Doris Dornak and Heath Roddy. If you have any questions, concerns or would like training on using your campus/classroom website, please contact Heath Roddy.

Technology Integration Support

The Assistant Director of Technology/Integration Specialist supports all technology integration for administrators, teachers and students. This includes professional development, coaching/modeling in the classroom, Tech Tips, Blended Learning support, and guidance through PLCs or other related needs on campus related to the curriculum and technology.

The Assistant Director of Technology/Integration Specialist collaborates with teachers and district leaders to create student-centered lessons that incorporate technology as a tool to ensure our students gain 21st Century skills. Teachers can request support through our Tech Ticket system. Support includes modeling, co-teaching, and professional development. This includes one to one, small group/teams/departments, or whole campus.

If you need assistance integrating technology in the classroom or an individual to brainstorm new ideas for use of technology, please fill out a tech request and the Assistant Director of Technology/Integration Specialist will schedule a support time.

New Staff & Faculty

All new staff and faculty will be given an introduction training on designated days. Training will include introduction to various systems such as:

- Logging in to network
- Accessing Google Drive

Technology

Heath Roddy, Director of Technology, 979-488-2595

- Accessing web based resources such as TEKS Resources, DMAC, Teacher webpage, inputting a Tech Ticket
- Signing Teacher AUP

Email/Network Account

All new staff must read and complete the E-mail/Network Account application. Included in this procedural guide is the "Acceptable Use Policy of Information Technology Resources". All applicants must also confirm that they have read and agree by signing and dating the document.

This application is available online at **https://tinyurl.com/ybd4aboq**

Human Resources will submit the following information to the Technology Department staff requesting a new WISD Network Account.

All email passwords will now be changed every 60 days as a security measure.

Information to include:

1. Legal Name of Employee
2. Office /Grade Level Assigned
3. Campus Assigned.

Substitute Teacher Network Access

Substitute teachers are **NOT** given access to Wharton ISD network for classroom instruction.

Long-term subs are given their own username/password and access to the Wharton ISD network including email. However, they will **NOT** receive their credentials until an AUP is signed and on file with the Technology Department. In those instances the username/password has to be shared, the Technology Department can unlink a teacher's password/account from their email and Google Drive password before they share it with a long term sub.

Guest Account Access

WISD offers a generic guest account for visitor and presenter use only. It is a limited account that only provides temporary access to the internet. If you need help with this, please contact the Technology Department.

Existing Positions

Newly hired personnel into existing positions shall receive the same workstation as the employee leaving that position unless the Director of Technology indicates otherwise.

Technology

Heath Roddy, Director of Technology, 979-488-2595

Transfer Employees

Employees that transfer from one department of another shall receive a workstation from the Department that the employee is moving into. If the employee is moving within the Department, it is at the discretion of the Director of Technology whether the workstation follows the employee.

New Positions

Employees hired into newly created positions shall receive a temporary workstation or laptop (if available) to utilize until the Director of Technology can purchase or locate the employee a new workstation.

District Technology Use in Wharton ISD

Use at Home

Hardware distributed to staff or students is the property of Wharton ISD. If students needs to take a device off of District property, prior approval needs to be given from the Director of Technology so proper monitoring/filtering software can be added and then checked out to the student or staff by the campus Librarian.

Use at School/District

Hardware is to remain in the assigned room. If hardware needs to be moved, campus principal must give permission and then the hardware must be "digitally moved" by campus Librarian. Hardware is assigned to a specific user should not be moved without following the proper channels.

Device Missing or Broken

If a device is broken, stolen or lost it please contact the Director of Technology IMMEDIATELY. You'll also need to fill out the loss/damage/stolen form. Form: **https://tinyurl.com/ycjahzov**. This form can be found on the district website under the Technology Department. In addition, if the item is stolen, contact the campus principal and Officer Williams so a police report can be filed.

Software

Wharton ISD has general software loaded on to their computers: Microsoft Office, Google Chrome. If there is other software you would like installed on your computer, please submit a service desk ticket. Software must be approved by the Technology Director and has to be installed by a member of the IT staff. The installation of personal software is not allowed on district devices. Software for textbooks not currently being utilized by a teacher cannot be installed on any computer. This would be a licensing violation.

Technology

Heath Roddy, Director of Technology, 979-488-2595

Computer Labs

All campuses have a student computer lab. If specific software is needed by teachers for use in the lab, it will be installed, after approval, by the IT staff. Each campus is responsible for keeping these labs running properly and informing the IT department in the form of a Tech Ticket if problems arise.

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.

Suspension or Termination of a Network 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. All request for suspension or termination of account will come from the HR department directly to the Director of Technology.

Data Security

As part of your duties, you may have access to confidential information. Caution must be taken to ensure this data is not exposed to those without a need to know. A data file containing confidential information that is released can damage the financial or professional futures of others, thus this information must be handled appropriately.

- Limit data exports to only the necessary information on the required people.
- Do not leave data files or computer equipment in an unsecure location such as an unattended automobile.
- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day. When they are expected to be gone from their office, they need to be sure confidential information is secured in a locked drawer or location when the area is unoccupied.
- Printouts containing confidential information should be immediately removed from the printer.

Technology

Heath Roddy, Director of Technology, 979-488-2595

- Upon disposal, confidential information should be shredded using District shredders. Whiteboards, etc. containing sensitive information should be erased after use.
- Lock up portable computing devices including laptops, external drives, and flash drives.
- Access to confidential information should be given on an as needed basis. If you are able to access confidential information that you do not need, you are required to report it to the manager of that data system.
- Be very cautious in transporting data files. Data transported on flash drives or external drives can be lost easily.
- Cloud based storage systems such as PERSONAL Google Drive and Dropbox are also susceptible to leaks especially if users do not correctly configure sharing permissions. Therefore, be sure you are using a Wharton ISD account to protect confidential information.
- All confidential information should be stored on District access controlled network storage.
- Data files containing confidential information that are leaving the District via email or on media should be encrypted (contact the Technology Department for assistance).

Content Filter

WISD as web filter to helps detect, identify, analyze and prevent attacks to our network. Because of web filter, the devices will easily authenticate on our network that will prevent sites from getting blocked. If you experience a site that is blocked, please fill out a Tech Ticket and the Director of Technology will evaluate the site, then unblock if deemed appropriate. The WISD web filter will also work on devices that are taken home and monitor those devices for security purposes.

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". Use of any proxy server to bypass the WISD Content Filter (as required by the Children's Internet Protection Act- CIPA) is considered a serve violation and user may receive disciplinary action. 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. Bypassing district filters and security via proxy servers, VPN Access or other means will NOT be tolerated and will be considered a violation of the WISD Acceptable Use Policy.

Barracuda

Most cyber-attacks start with a targeted email leading to significant financial damage and data loss. Barracuda provides a layer of protection of all aspects of WISD email infrastructure to protect our network and user data. If email arrives in your inbox that looks "suspicious" please delete the email and let the Director of Technology know. In addition, if you are experiencing password issues or issues with emails getting caught in Barracuda, whitelist these emails or let the Director of Technology know. Please read the following passages regarding electronic mail.

Technology

Heath Roddy, Director of Technology, 979-488-2595

Electronic Mail:

Email has become one of the most used communications tools in the home and workforce. The following guidelines must be understood and adopted into your daily operation:

- **Electronic mail is a privilege, not a right.** User responsibilities and consequences for policy violations apply to email as well as other communication devices (i.e., desk phone, cell phone, two-way radio, etc.).
- **Public Information Act**. The software and hardware that provides us email capabilities has been publicly funded. For that reason, it should not be considered a private, personal form of communication.
- The contents of any email communications are governed by this Acceptable Use Policy and subject to the Public Information Act. The District must comply with any legal requests for access to email contents.
- **Misaddressed emails**. Incoming email that is misaddressed will remain "undeliverable". It is your responsibility to ensure you give out your correct email address.
- **Release of Student Records**. No request for student grades, discipline, attendance or related information can be communicated via email unless a signed Release of Student Records is on file on the campus.
- **Personal emails**. Personal email should not impede the conduct of District business; only incidental amounts of employee time (time periods comparable to reasonable coffee breaks during the day) should be used to attend to personal matters. Employee time may be restricted by supervisor or campus administrator.
- **Avoid phishing scams**. Phishing email will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has.
- **Records Retention**. Each employee shall comply with the District's requirements for records retention and destruction to the extent those requirements apply to electronic media.
- **No official business using third-party email**. Users are prohibited from using third party email and storage servers to conduct Wharton ISD business. Such communications and transactions should be conducted through proper channels using Wharton ISD approved methods. Personal email accounts used to conduct District business may be subject to Public Information Requests.
- **No expectation of privacy**. Users should have no expectation of privacy in anything they store, send, or receive on the District's email system. Messages may be monitored without prior notice.
- **Email addresses** are assigned at the discretion of the Technology Department based on a user's legal name. In some circumstances it may be necessary to change your email address. Technology can assign a new address at its discretion.

Telephone

Telephone communication is an essential part of the day-to-day operations of Wharton ISD. Telephone and voicemail services are provided to employees of Wharton ISD to facilitate performance work. Since our phones require internet access, in the event we lose internet, the Technology Department will have the main line from each campus routed to the campus fax line. If this happens, the following procedures will take place:

1. Once the Technology Department identifies if an issue can't be fixed in a timely manner, the Technology Department will notify the Superintendent, Deputy Superintendent and Assistant
2. Inform the Superintendent that emergency phone procedures will be put in place.
3. The Technology Department will send a text to each principal informing them of the problem and requesting that Emergency Phone Procedures be put in place on each campus.
4. The technology Department will call Mitel and have all main phone extensions forwarded to the each department fax machine. **(Please understand, once we put emergency phone procedures in place, the process of transferring direct numbers to fax lines can take up to 45 minutes.)**
5. The Technology Department will inform campus principal that phones have been restored to original settings.

Please remember:

- If the internet goes down, the Technology Department is aware of the problem. Having multiple individual's call the Director of Technology's cell only slows down the process.
- If the internet connection is restored, someone still needs to "man" the fax line until the Technology Department informs each campus that phones have been reverted to original settings.

Individual Phones

If you have been assigned a phone, it is up to you to change the voicemail message from the previous owner. To do this, please follow the steps below.

When you dial 6000 on your phone, you will get a message to enter your passcode. The passcode to all new employees is 1111.

You will hear "You have 0 messages or you have # messages."

- Press 7 to play first message
- Press 9 to exit system

To make changes to your message, greeting or name: Dial 6000 then press 8. (Change user options)

- Press 6 to make message new message
- Press 4 to change greeting
- Press 6 to change the name
- Press 7 to change passcode
- Press 9 to exit the system

Printers

Any individual needing their computer mapped to a certain printer or Xerox printer, please fill out a Tech Request. Please provide the name of the printer you wish to print to as well as the IP address to your computer. The IP address to your computer can be found on the lower right hand corner of the task bar. Please hover your mouse over the green/red icon to get the IP address. It should read something like: 172.21.?.??. The Technology Department will need an address to assist you will your issue. The technology department does **NOT** support personal printers on the WISD network. The technology departments does **NOT** purchase ink for campus printers or replacement parts.

Technology

Heath Roddy, Director of Technology, 979-488-2595

Assets Disposal

Any hardware that is no longer in use needs to be assessed by the Technology Department. Put in a Tech Ticket for item(s) to be picked up.

Technology Availability

The District's technology 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.

Social Media in Wharton ISD

Personal Internet Postings/ Social Media Sites:

Social media also includes all forms of telecommunication such as landlines, cell phones, and web-based applications. Employees are encouraged to maintain separation between personal and professional postings for Social Media Sites. Conduct on social media sites is governed by Board Policy DH (Local).

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 social media as they are for any other public conduct.

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.

Technology

Heath Roddy, Director of Technology, 979-488-2595

Employees are not required to provide students with their personal phone numbers or email address.
Texting should not occur between 9:00 p.m. and 6:00 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.

Technology

Heath Roddy, Director of Technology, 979-488-2595

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 Use of Social Media

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.

Purchasing (This includes DonorsChoose grants related to technology)

If purchasing technology through campus or department budget, grant or any other funding, contact the Director of Technology **PRIOR** to purchasing. If writing a grant, contact the Director of Technology before applying. This ensures the hardware or software you are purchasing works with our existing network. **The Technology Department must be consulted prior to any purchase of hardware or software. If hardware or software is given the "green-light" by the Director of Technology, all items purchased that requires setup must be shipped to the Educational Support Center for setup and inventory purposes. If software**

is found on a computer and there is no license, the Technology Department will uninstall said program until documentation can be produced.

DonorsChoose

WISD certainly encourages the grant writing practice. However, if a grant is to be written, grant writers must fill out a form found on the Wharton ISD website then turn this into their campus principal. The campus principal will then sign form then send to the ESC for more signatures.

Computer Software Purchases:

Our goal is to promote the use of appropriate and approved software whenever possible. These guidelines will ensure that the required support and installation process is in place before funds are expended. To ensure that software will not affect the current network configuration adversely, the following guidelines apply when you want to purchase software.
All software purchases must be purchased through and delivered to the Technology Department for installation.

- Contact the Director of Technology prior to purchasing.
- Software will be installed only when there is documentation showing that the software purchase has gone through the process referenced above and that proper licensing has been purchased.
- Only Technology staff or an authorized vendor shall install computer software on District computers.
- If a software program is determined to be unsuitable for the network or current environment it **WILL not** be purchased.
- An invoice of software purchase will be sent to the Director of Technology for record retention.

Computer Hardware Purchases:

The authorization process includes testing of hardware for compatibility and functionality.

- All hardware must be purchased through and shipped to the Technology Department with documentation listing campus name and contact.
- Campus computer systems may not be modified, upgraded, or replaced with donated equipment without the prior approval of the Director of Technology.
- To maintain accurate physical inventory, desktop computer systems should not be moved from one campus to another without prior
- Approval of the campus principal as well as the campus Librarian for inventory purposes. However, the Director of Technology must be notified of the move.

1:1 Chromebook Initiative

The Wharton Independent School District has established a 1:1 Chromebook Initiative for all 7th and 8th grade students at Wharton Junior High. Although these devices will be used during school hours only, the goal is to eventually work towards a "take-home" model for both grade levels. These devices will be

Technology

Heath Roddy, Director of Technology, 979-488-2595

filtered using Content Keeper and GoGuardian management software. These devices are the property of WISD and subject to all rules and regulations established by Board Policy as well as those written in this guide and in the student AUP.

Personal Devices

No personal devices to the Wharton Independent School District will be supported by the Technology Department. These devices, if on school network for personal use or for training purposes, will not be allowed to properly authenticate, therefore; the user will experience sites being blocked.