This handbook is being provided to the Waco Independent School District in an effort to inform, educate, and standardize practices involving technology.

This handbook will be updated as needed to reflect any new technologies and/or procedures.
# Table of Contents

Mission & Vision .................................................................................................................. 4
Acceptable Use Agreement (Staff and Students) & Internet Safety ........................................ 5
Password Guidelines ............................................................................................................. 12
Email Guidelines ................................................................................................................. 13
Active Directory .................................................................................................................. 16
Computer Power off Guidelines ........................................................................................... 16
Copy Machines .................................................................................................................... 16
Disaster Recovery Plan ....................................................................................................... 17
Donated Technology Equipment and/or Software Guidelines ................................................. 17
Electric Pencil Sharpeners .................................................................................................... 17
Equipment Disposal Guidelines ........................................................................................... 18
Google Classroom & Student Emails .................................................................................... 18
Hardware & Software Purchasing Guidelines ........................................................................ 19
Hardware Movement .......................................................................................................... 19
MDF & IDF ROOMS: .......................................................................................................... 20
Mobile Tablets ....................................................................................................................... 20
Network drop requests ........................................................................................................ 20
Obtaining Quotes for Technology Hardware ......................................................................... 21
Physical moving of equipment .............................................................................................. 21
Remote Access to Computers ............................................................................................... 21
Scheduled Network Outage ................................................................................................. 21
Security Cameras .................................................................................................................. 21
Separating Employees ......................................................................................................... 23
Substitute Teachers ............................................................................................................. 23
Unanticipated Network Outage Communications ................................................................. 23
Work Tickets ....................................................................................................................... 24
Technology Department Staff ............................................................................................... 25
Technology Tips and How Tos ............................................................................................. 26
   How To Set Up Your Active Directory Account ................................................................. 26
   BYOD: Connecting Your Personal Windows 8 Device to the WacoISD Network ................. 26
   BYOD: Connecting Your Personal iOS Device to the WacoISD Network ......................... 26
   BYOD: Connecting Your Personal Android Device to the WacoISD Network .................. 26
   What is this W Drive? ....................................................................................................... 26
Mission & Vision
The Waco Independent School District (WISD) Technology Department strives to develop and maintain a network and customer client support that provides reliable service to all district staff.

The focus is to develop a customer service infrastructure that continually seeks to understand and meet customer requirements. As part of this effort, the following mission and vision statements have been developed.

Mission
To integrate appropriate technology into the educational environment to promote the use and application of various technological tools needed in modern society for the full development of competence in both students and staff.

Vision
To be a knowledgeable, customer-focused, empowered, and professional team that continually learns and improves its effectiveness.

Provide access to information in its past, present, and future forms with multimedia, multi-sensory methods that are powerful, easy-to-use, and increasingly reduce the constraints of time and space.
Acceptable Use Agreement (Staff and Students) & Internet Safety

WACO ISD
Electronic Communication Systems

Employee and Student
Acceptable Use Agreement (AUA) and Internet Safety

Please read the following information carefully.

This is a legally binding document for students and employees of Waco Independent School District. The most updated version can be found at wacoisd.org/aua

I. OVERVIEW

The Waco Independent School District Network (WISD network) offers students and employees (here in referred to as WISD members) access to the District’s Electronic Communication System for educational purposes. Our goal is to promote educational excellence in the Waco Independent School District by providing effective and meaningful classroom instruction and administrative needs while ensuring a safe, ethical and productive learning environment. With this educational opportunity comes responsibility.

**Definition of District’s Electronic Communication System**: The District’s computer systems and networks are any configuration of hardware and software. The system includes, but is not limited to the following:

- District provided cellular telephones, and voicemail technologies;
- Email accounts;
- Servers;
- Computer hardware and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, email, digital images, and video and audio files;
- Internally hosted or externally hosted databases, applications, tools (Internet or District server based);
- District-provided Internet access;
- District-filtered public Wi-Fi;
- Virtual environments; and
- New technologies as they become available
**Definition of a computer system account:** any login and password information disseminated to WISD members for the purpose of enrolling into a computer program, whether it is hosted in the district or off-premises. A computer system account is not limited to: Active Directory (AD), Eduphoria, TEAMS, Milestone Camera systems, login to a non-/domain district computer, ID camera software, accounts established to manage online learning programs (such as, but not limited to, Lexia, Successmaker, iStation, and others).

It will be the user's responsibility to follow the rules for appropriate and acceptable use.

The Internet is a network of many types of communication and information networks. With access to computers and people all over the world comes the availability of adult content or material that may be considered objectionable and may not be considered to be of educational value in the school setting. In compliance with the Children’s Internet Protection Act (CIPA), the school district has installed active content filtering and/or blocking software to restrict access to Internet sites containing material harmful to minors.

While the District uses filtering technology and protection measures to restrict access to such material, it is not possible to absolutely prevent such access. A user who incidentally connects to an inappropriate site must immediately disconnect from the site and notify a teacher/administrator. If a user sees another user accessing inappropriate sites, he or she should notify a teacher/administrator immediately.

In addition, access to the electronic communication system is a privilege, not a right. The smooth operation of the network relies upon the proper conduct of all users who must adhere to strict guidelines. These guidelines are provided in this document so that you are aware of the responsibility to follow the rules for appropriate and acceptable use you are about to acquire. In general, this requires efficient, ethical, and legal utilization of the network resources. Noncompliance may result in suspension of access or termination of privileges along with other appropriate disciplinary action consistent with Waco ISD Policies. All WISD students are required to abide by the Student Code of Conduct. All WISD employees are required to abide by the Code of Ethics and Standard Practices for Texas Educators (“Code of Ethics”), State and Federal law, and District Policy. All users must abide by ethical standards when communicating with WISD members, regardless of whether such communication takes place on campus, during instructional time, through use of the System or not. Violations of law may result in criminal prosecution as well as disciplinary action by Waco ISD.

II. PHILOSOPHY

   a. **Risk** – Even with filtering, blocking, and anti-virus software, controlling all materials on the WISD network is impossible. Sites accessible via the WISD network may contain material that is illegal, defamatory, inaccurate or harmful. With global access to computers and people, a risk exists that users may access material that may not be of educational value in the school setting.

   b. **User Responsibility** – WISD network users, like traditional library users, are responsible for their actions in accessing available resources. Should inappropriate materials become available, users must notify a campus teacher/administrator and/or district system administrator immediately.

III. TERMS AND CONDITIONS

**Responsible Use:** Waco ISD Electronic Communication System (WISD network) access may be used to improve learning and teaching consistent with the educational goals of Waco ISD. Waco ISD expects legal, ethical, and efficient use of the WISD network. District-approved email accounts will be provided for WISD members based on district initiatives. District-approved social media activities that are educationally related may be used. **At no time should personal use of Waco ISD’s Electronic Communication System (WISD network) come in conflict or hinder a user’s expected responsibilities.**

   a. **Privilege:** Use of a personal Waco ISD Network account is a privilege, not a right.
b. **Limited personal use** is permitted as long as it does not increase the cost to the District or interfere with the operations of the network. The District will provide a filtered, wireless public network to which staff will be able to connect personal telecommunication devices for instructional and administrative functions. These devices are the sole responsibility of the staff owner. The campus or District assumes no responsibility for personal telecommunication devices if they are lost, loaned, damaged or stolen and only limited time or resources will be spent trying to locate stolen or lost items. Each WISD member is responsible for their own device; set up, maintenance, charging and security. District staff will not diagnose, repair or install software on another member’s device. Should inappropriate activities or a security breach be detected, appropriate District staff may examine the staff member’s device.

c. **Subject to System Administration:** All Waco ISD Network accounts and computer usage are subject to perusal by the system administrator for virus scanning and monitoring for inappropriate use and investigation of suspected misuse at the authorized direction of Campus or District administrations regardless of cause. All District computer/network/Internet usage shall not be considered confidential. WISD members should not use the computer system to send, receive or store any information, including email messages, they consider personal or confidential and wish to keep private. All electronic files, including email messages, transmitted through or stored in the computer system will be treated no differently than any other electronic file. The District reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. WISD members should treat the computer system like a shared or common file system with the expectation that electronic files, sent, received or stored anywhere in the computer system, will be available for review by any authorized representative of the District for any purpose. Personal telecommunication devices are subject to examination in accordance with these guidelines.

d. **Required Training:** All WISD members will participate in annual training for appropriate technology use, as required by the district.

IV. **INAPPROPRIATE USE:** Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations by Waco ISD, that violate the rules of network etiquette, or that hamper the integrity or security of Waco ISD’s electronic communication system.

a. **Violation of Law:** Transmission of any material in violation of any U.S. or State law is prohibited. This includes, but is not limited to: copyrighted material; threatening, harassing, or obscene material; or material protected by trade secret. Any attempt to break the law through the use of a WISD network account may result in litigation against the offender by the proper authorities. If such an event should occur, Waco ISD will fully comply with the authorities to provide any information necessary for the litigation process.

b. **Commercial Use:** Use for commercial, income-generating or “for profit” activities, product advertisement, or political lobbying is prohibited.

c. **Vandalism/Mischief:** Vandalism and mischief are prohibited. Vandalism is defined as any malicious attempt to harm or destroy data or devices of another user, the WISD network, or any other networks that are connected to the WISD network. This includes, but is not limited to, the creation or propagation of computer viruses. Any interference with the work of other users, with or without malicious intent, is construed as mischief and is strictly prohibited.

d. **Electronic Mail Violations:** Forgery of electronic mail messages is prohibited. Reading, deleting, copying, or modifying the electronic mail of other users is prohibited. Sending unsolicited junk mail, spam, chain e-mails, or that of commercial content is prohibited. Using accounts (including the signature files) for non-school related activities including but not limited to: financial gain, pornography/child pornography, personal advertising, buying, or selling political activities including lobbying public relations, activities such as solicitation fundraising religious activities is prohibited.
e. **File/Data Violations:** Deleting, examining, copying, or modifying files and/or data belonging to other users is prohibited.

f. **System Interference/Alterations:** Attempts to exceed, evade or change resource quotas are prohibited. Installing unauthorized network access points or other connections, causing network congestion through mass consumption of system resources, attempts to disable the WISD network filter or compromising the integrity of the firewall are prohibited.

g. **Inappropriate Speech/Messages:** The following restrictions against inappropriate speech and messages apply to all communication sent and/or accessed through WISD network, including all e-mails, instant messages, texts, web pages, blogs, wikis, or other avenues of electronic communication. Users shall not send obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful messages. Users shall not post information that could cause damage, danger, or disruptions, or engage in personal attacks, including prejudicial or discriminatory attacks. Users shall not harass another person or knowingly or recklessly post false or defamatory information about a person or organization. Personal, political use to advocate for or against a candidate, office holder, political party, or political position. Research or electronic communications regarding political issues or candidates shall not be a violation when the activity is to fulfill an assignment for class credit.

h. **Home/Personal Internet:** A user’s home and personal electronic communication use can have an impact on the school and on others. A user’s personal electronic communication expression, including but not limited to, a threatening message, a violent or sexual web site, a text, or a post that creates a likelihood of material or substantial disruption of the school/district’s operation may result in district disciplinary action and/or criminal penalties.

i. **Bullying/Harassment:** Our district takes cyber bullying and harassment by electronic communication very seriously, and it will not be tolerated. Users shall not use any Internet or other communication device to intimidate, threaten, bully, harass, or embarrass students or WISD members. Users who engage in such activity on school grounds or who engage in such activity off campus and create a material or substantial disruption of school operations (or the reasonable potential exists) shall be subject to disciplinary actions as well as possible criminal penalties.

V. **CONSEQUENCES OF AUA VIOLATION:** Any attempt to violate the provisions of these procedures will result in revocation of the user’s account, regardless of the success or failure of the attempt. In addition, students may face district disciplinary action (Student Code of Conduct) and/or appropriate legal action. In the event of a claim that a student has violated these guidelines, the district will provide the student with notice and an opportunity to be heard in the manner set forth in the Student Code of Conduct. Staff members may face district disciplinary action up to and including employment termination and/or appropriate legal action.

a. **Final Determination:** The Superintendent or the designee will make the final determination as to what constitutes inappropriate use.

b. **Denial, Revocation, or Suspension of Accounts:** The Superintendent/designee, departmental Director, campus Principal, and/or the System Administrator in accordance with Waco ISD disciplinary procedures may deny, revoke, place restrictions, or suspend an account.
VI. SECURITY


b. Reporting Security Problems: If a user identifies or has knowledge of a security problem on the WISD network, the user must notify a teacher, campus principal, system administrator, and/or the Superintendent’s designee for Waco ISD. The user shall not reveal or demonstrate the problem to others. Any user who attempts or causes a breach of system security may have his/her privileges revoked and may be subject to additional disciplinary and/or legal action.

c. Impersonation: Attempts to login to the WISD network as a system administrator or any other user may result in suspension of access to the District’s electronic communication system as well as other appropriate disciplinary or legal action in accordance with the Student Code of Conduct or board policy.

d. Security Risks Denied Access: Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the WISD network.

e. Supervision: Staff must supervise student use of the District’s electronic communication system in a manner that is appropriate to the students’ age and the circumstances of use.

f. Filtering Software: Users may not disable the District’s filtering software at any time. Authorized staff may temporarily or permanently unblock access to sites containing appropriate material if the filtering software has inappropriately blocked access to such sites.

g. Bandwidth: Bandwidth utilization is monitored. Users who routinely monopolize excessive amounts of bandwidth will be notified and their usage will be examined. In order to protect and reserve bandwidth and other resources for educational use, users may not:
   i. Download software or files that are not for educational purposes.
   ii. Play interactive online games.
   iii. View non-curriculum based streaming videos/movies.
   iv. Set their Internet browser home page to a digital media rich site (i.e. CNN, Yahoo, MSN).

VII. INTERNET SAFETY: Internet safety of WISD members in their use of the District's Electronic Communication System is a high priority.

a. NEVER give your username/password to anyone.

b. NEVER tell anyone online your full name, home address, phone number, age, friend’s name, your school, or any other personal information.

c. NEVER share photos of yourself, your family, or your home with people you meet online.

d. NEVER open attachments or click on links in an e-mail from someone you do not know.

e. NEVER make appointments to meet people whom you meet online. Students should report to a teacher or administrator if they receive such a request. Users who view Inappropriate Use, defined above, including but not limited to bullying/harassment or inappropriate speech/messages should not respond. A teacher or administrator should be notified immediately.

f. Do not accept e-mails, files, or web page addresses (and the like) from strangers. People who you meet online are not always who they say they are. Be aware that online information is not necessarily private.
DISCLAIMER

Waco ISD makes no warranties of any kind, whether expressed or implied, for the service it is providing and is not responsible for any damages suffered by the users. This includes loss, theft, or damage to personal devices; loss of data resulting from delays, non-deliveries, mis-deliveries; intrusion by computer virus; or other service interruptions or malfunctions. Waco ISD is not responsible for phone/credit card bills or any other charges incurred by users. Use of any information obtained via the WISD network is at the user's own risk.

Waco ISD is not liable for an individual’s inappropriate use of the District’s electronic communication systems or violations of copyright restrictions or other laws or for costs incurred by users through use of Waco ISD’s electronic communication system.

Responsible Use and Digital Citizenship

Respect Yourself: I will select online names that are appropriate, and I will be polite and use appropriate language/content in all online posts.

Protect Yourself: I will not publish personal details, contact details, or a schedule of activities for myself or anyone else. I understand that unless otherwise authorized, I am the owner of my accounts, and I am responsible for all activity initiated by and/or performed under these accounts. I understand that it is my responsibility to appropriately secure my account credentials. I understand that I am responsible for maintaining and backing up all of my own data. If I am uncertain whether a specific computer activity is permitted or appropriate, I will ask a teacher/administrator before engaging in that activity.

Respect Others: I will not use technologies to bully or tease other people. I will not make audio or video recordings of students/employees without their prior permission. I understand that posing as someone else is forbidden and I will not pose as a user other than myself when online. I will be careful and aware when printing to avoid wasting resources and printing unnecessary items.

Protect Others: I will help maintain a safe computing environment by notifying appropriate campus officials of inappropriate behavior, vulnerabilities, risks, and breaches involving campus technology.

Respect Intellectual Property: I will suitably cite any and all use of websites, books, media, etc. I will respect all copyrights.

Protect Intellectual Property: I will request to use the software and media that others produce.
The Acceptable Use Agreement of electronic communication facilities and services direct and require that all users:

1. Respect all Internet safety practices including online behavior, ethics, and netiquette.

2. Respect the legal protection provided by copyright and licenses to programs, applications, and data.

3. Respect the rights of others by complying with all present and future WISD policies regarding privacy and intellectual property.

4. Respect the rights of others by complying with all present and future WISD policies regarding sexual, racial, and other forms of cyber bullying and harassment and by preserving the privacy of personal data accessed.

5. Respect the privacy of others by not tampering with their personal devices, files, storage devices, passwords, and/or accounts in any manner.

6. Respect storage limits. Limit storage on the network to educational materials. Users will be assigned a fixed amount of storage. Users will be required to routinely review and purge unwanted and unneeded files.

7. Respect the integrity of computing systems and data, including but not limited to, infiltrating a computer system, damaging and/or altering the software or hardware components of a computer, and/or gaining unauthorized access via the network.

8. Respect the ethical standards set forth by the school district by using technology in a manner which is consistent with those standards and in a manner consistent with their intended purpose.

9. Respect and adhere to local, state, or federal law which may govern the use of technology in Texas and in the United States of America.

Acceptable Use Agreement Acknowledgement Form

I understand that my technology use and, if applicable, text messaging and social media with District provided resources, are not private and may be viewed by district officials. Any third party accounts that I use for educational purposes must also adhere to these Acceptable Use Agreement. I understand that the Waco Independent School District will monitor my activity on the computer system.

I have read the Waco ISD Acceptable Use Agreement for technology and agree to abide by their provisions. In consideration for the privilege of using the Waco ISD electronic communications system and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, including, without limitation, the type of damages identified in the District's policy and administrative regulations.
**Password Guidelines**

The WISD network is configured so that each staff member and student using the network is required to have a unique password and user-id also known as Active Directory (AD) credentials. This configuration allows the WISD network to handle a wide variety of complex tasks in a very secure way. However, this security depends upon the users’ participation. The following are security practices for staff users of the WISD network.

1. **Passwords are set to change at least every 12 months.** While the user-id will always remain the same, the password will have to be changed every 12 months from either the date of new employee orientation for employees hired in the last two years, or the date that the password was set up for employees with 2+ years of seniority. The system will prompt user at 15 days prior to the expiration on a Windows machine that has been imaged (AD Credentials required to login on the machine). If password is not changed before it expires, the user will need to login to a Windows machine that has been imaged and use the combination CTRL-ALT-DELETE keystroke and select Change Password.

2. **Choose A Good Password.** Passwords must contain a minimum of 8 characters and adhere to the following: Not contain user's account name or parts of user's full name that exceed two consecutive characters; Not contain spaces; contain an English uppercase character (A-Z); contain an English lowercase character (a-z); contain at least one number (0 through 9); contain at least one non-alphabetic character (For example !, $, @ or #). In addition, the password must be a unique in that it cannot be one of the last (8) eight passwords used. Users should select a password that is easy to remember, but which is difficult to guess. Users should avoid using last name, or other simple-to-guess words as a password. Passwords should not be selected merely on fact that they are easy to type as these passwords are easily guessed.

3. **Never Share A Password.** Each and every staff user will have his or her own password that is not to be shared with any staff member, including administrators, and/or administrative assistants. The user-id can be used to track system activity and therefore only the actual user associated with the password should ever use it. **Allowing another person to use a login & password does not remove the owner from any responsibility for any actions taken with the shared credentials.**

4. **Do Not Store Your Password In Function Keys, Macros, or Web Browsers.** This action seriously degrades the security of the WISD Network. There is a high potential for miss-use of the system when user –id and passwords can be obtained from function key or macro programming.

5. **Do Not Leave Your Workstation In Secured Modules.** If you have used your password to get into one of the secured modules (TEAMS, First Class), it is important that you exit back out of that area before leaving your session running unattended. On Windows machines, using the combination of Windows-Flag and L will lock your computer.

6. **COMPROMISED PASSWORD.** If you feel an account or password is compromised, report the incident to the Technology Help Desk (755-9599 or helpdesk@wacoisd.org) and your password will be reset.

7. **VIOLATIONS.** Any employee found to have violated this policy may be subject to actions up to and including loss of access to network resources and disciplinary action.
**Email Guidelines**

Users are reminded that all uses of the Waco ISD's information technology resources, including electronic mail, are subject to all relevant Waco ISD policies and relevant state and federal laws, including federal copyright law.

Appropriate use of Waco ISD electronic resources includes instruction, research, service, and the official work of the offices, departments, recognized student and campus organizations, and as described below, incidental personal usage by faculty, staff, and students. Since resources are not unlimited, the district may give priority for resources to certain uses or certain groups of users in support of its mission. Consistent with the district's non-discrimination policy, the use of information resources should not be denied or abridged because of race, creed, color, sex, sexual orientation, religion, national origin, age, or physical disability.

Use of electronic mail for all school and school district business by staff members must be conducted using an approved program and district domain. Currently, the approved email program is *FirstClass* by *OpenText*.

**Account Details**

All email accounts will be assigned by the Waco ISD Technology Department. Email storage size will be limited to 200MB. If additional storage is needed, that request must be submitted in writing to the Technology Help Desk for approval. It is the responsibility of each individual to manage his or her email account; this includes archiving, organizing and deleting emails. Email accounts should not be used to store files (documents, pictures, etc.). The W drive that is available to all staff members should be used for this purpose. In situations where the W drive is unavailable (example – ConnectED campuses, the File Storage folder in First Class can be used to store any documents that contain student/staff confidential information).

**Privacy of Email Files**

Waco ISD encourages the use of electronic mail and respects the privacy of users. It does not inspect or monitor electronic mail routinely, nor is the district responsible for its contents. Nonetheless, users of electronic mail systems should be aware that, in addition to being subject to authorized access as detailed below, electronic mail in its present form cannot be secured and is, therefore, vulnerable to unauthorized access and modification by third parties. Receivers of electronic mail documents should check with the sender if there is any doubt about the identity of the sender or the authenticity of the contents, as they would with print documents. Users of electronic mail services also should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there may be back-up copies of such electronic mail that can be retrieved on the district systems or any other electronic systems through which the mail has traveled.

Waco ISD electronic mail services may, subject to the foregoing, be used for *incidental personal purposes* provided such use does not interfere with Waco ISD operation of information systems.
technologies including electronic mail services, burden the Waco ISD with incremental costs, or interfere with the user’s employment or other obligations to the district. Access by authorized Waco ISD employees to electronic mail stored on the district’s network of computers may be necessary to ensure the orderly administration and functioning of the district’s computing systems. Such access, gained for purposes such as to back up or move data, ordinarily should not require the employee gaining access to the electronic mail to read messages. Waco ISD requires employees, such as system administrators, who as a function of their jobs routinely have access to electronic mail and other electronically stored data to maintain the confidentiality of such information.

Access to electronic mail on the district’s network of computers that involves reading electronic mail may occur only where authorized by the Waco ISD officials designated below and only for the following purposes:

- Troubleshooting hardware and software problems, such as rerouting or disposing of undeliverable mail, if deemed necessary by the Technology Director or his or her authorized designee;
- Preventing or investigating unauthorized access and system misuse, if deemed necessary by the Technology Director;
- Investigating reports of violation of Waco ISD policy or local, state, or federal law;
- Investigating reports of employee misconduct;
- Complying with legal requests for information (such as subpoenas and public records requests); and
- Retrieving information in emergency circumstances where there is a threat to health, safety, or Waco ISD property involved. In addition to the foregoing, when a Waco ISD employee leaves employment or when a student graduates or otherwise withdraws from the Waco ISD, a system administrator may remove the departing employee’s or student’s email files from Waco ISD systems in order to conserve space or for other business purposes. An employee’s email may be retained and accessed by the campus or department as necessary for use in connection with Waco ISD business. A student’s email should be deleted unless otherwise required in connection with Waco ISD business. In all such cases the extent of the access will be limited to what is reasonably necessary to acquire the information for a legitimate purpose. Campuses and departments are encouraged to make arrangements for disposition of email files with departing employees and students in advance of their departure.
- Privacy of Data, other than Electronic Mail, Stored on Waco ISD Computers and Networks

In order to conduct its business without interruption, the district must have access to data stored on Waco ISD computers and networks. Accordingly, for legitimate business purposes, the Superintendent or designee may in his or her discretion authorize the accessing or retrieval of any files other than electronic mail stored on Waco ISD computers or other hardware where necessary and appropriate.

**Public Records Considerations**

Electronic mail and other data stored on Waco ISD computers may constitute a public record like other documents subject to disclosure under the Texas Public Records Act or other laws, or as a
result of litigation. However, prior to such disclosure, the district evaluates all requests for information submitted by the public for compliance with the provisions of the Act or other applicable law. All email will be stored on the Waco ISD servers for a time period of 30 days. Incidental personal electronic mail may be destroyed at the user's discretion.

**Posting to the NEWS Conference**

As a publicly funded system, postings that advertise for sale, for rent, are commercial in nature, etc., cannot be allowed, to include not-for-profit listings. Do not advertise personal for profit business or the businesses of others, no matter how small. Postings should pertain to the group or location identified. Only fund raisers approved for the benefit of WISD or its locations will be allowed. Messages in violation will be deleted without notification by authorized persons in technology.

**Conclusion**

Wherever possible in a public setting, individuals' privacy should be preserved. However, there is no guarantee of privacy or confidentiality for data stored or for messages stored or sent on Waco ISD-owned equipment. Persons with questions about the applicability of this Policy to specific situations should contact the Waco ISD Technology Department.

Violations of Waco ISD policies governing the use of Waco ISD electronic resources, including mail services, may result in restriction of access to Waco ISD information technology resources in addition to any disciplinary action that may be applicable under other Waco ISD policies, guidelines or implementing procedures, up to and including dismissal. Suspected violations of Waco ISD Policy may be reported to the Waco ISD Technology Director.
**Active Directory**

Active Directory (AD) is a special-purpose database developed by Microsoft Corporation. The district utilizes the comprehensive program to maintain permissions based on roles in the district that tie into usernames based on assignments as determined by Human Resources on TEAMS. For the 2015-16 school year, students will have AD accounts generated by their active status on TEAMS. The AD username and password is used to gain entrance to hardware devices, TEAMS, Help Desk Ticket System (KACE), Milestone Camera Software, and other applications.

**Bring Your Own Wireless Device (BYOD)**

The District is fortunate to have a wireless (WiFi) infrastructure in which staff members are permitted to provision up to four of their personal devices on the network. Setup instructions can be found at [technews.wacoisd.org](http://technews.wacoisd.org) and at the end of this document at Technology Tips and How Tos. Please note that the Technology Department cannot provide support in managing your personal device. All network access usage is governed by the District’s Acceptable Use Agreement.

**Cloud and Ground Online Storage Options**

Staff members are afforded several options to save and retrieve files. Aside from the local hard drive, files can be saved in the Google Drive, W, or S Drive. The Google Drive has unlimited storage and files can be retrieved outside the District’s network. The W drive is available on Windows computers and is tied to the user’s Active Directory account. Files saved on the W drive can be retrieved from any computer in the district. The S Drive is available to save files that are meant to be shared with other users on the campus or building. For confidential files (containing student pictures, testing, contact information), use of the W drive is highly recommended as the hardware is located in the district and there is a lesser opportunity for a data breach. The W drive by default is set to 10GB of storage. Please contact the Technology Help Desk if your needs exceed that capacity.

**Computer Power off Guidelines**

All staff members are reminded to turn off the power to their desktop computers at the end of the workday (with the exception of the first Wednesday of every month). Please allow printers to remain powered on so as to not risk loss of identifier information on them.

Note the power is still on for a computer even when it is "asleep" or in “energy saving mode.” Switch the surge protector to "off" to ensure all power to the computer is disconnected. Exceptions: computers scheduled for automatic backup during the night, computers running critical processes at night, and computers explicitly configured for remote access. If you have a question on a computer you think might be running the universe and would like a second opinion on whether or not to turn it off, please feel free to contact our Help Desk at 755-9599.

**Copy Machines**

The approved contractor will provide services of district-leased copy machines. The Technology Department’s staff is involved with securing a Static IP address to the copier should the campus...
decide to use it as a printer. Other issues with the copier (including adding email addresses for scanning purposes) will need to be addressed with the approved contractor.

**Disaster Recovery Plan**

The purpose of the Waco ISD Disaster Recovery Plan is to provide for continuation of the information processing and telecommunications required supporting Waco ISD should a disaster occur affecting the necessary computing and telecommunications systems.

This plan provides recovery personnel with information required in implementing the disaster recovery effort. It provides the necessary information and procedures to facilitate the recovery from a disaster and to relocate computing and telecommunications equipment, if necessary, to a recovery center at the time of a disaster.

Disaster, system malfunction, or sabotage do not negate the District’s responsibility to produce attendance and/or financial data required for an audit. Waco ISD has a plan in place detailing how we will recover and reproduce data required for an audit if the original data source (hardware/software) is threatened by disaster or by system malfunction or sabotage.

**Financial Data:**
- **Historical Data:**
  - Through the years changes in hardware and software restrict our ability to easily access past year’s data. The data is backed up and secure but we would need to locate hardware and software to access it.
  - Starting in the 2010-2011 school year student data are stored and accessed through an SQL database. The data accumulates year to year and may be accessed from one location/system.
  - Multiple years of financial data is available online.

**Student Data:**
- Five copies of the data are made on a daily basis
- The copies are stored:
  - Offsite – replicated to a SAN housed in an offsite location.
  - Onsite – Data Center on a high availability SAN.

**Donated Technology Equipment and/or Software Guidelines**

All technology equipment and software that is being donated for use on the District’s computers and/or network must be certified by Technology Director as “compatible” with the minimum technology standards, and as “supportable” to ensure appropriate maintenance and repair.

**Electric Pencil Sharpeners**

The Technology Department is not responsible for the maintenance and/or service of these and other similar devices that require electrical current in order to function.
**Equipment Disposal\Transfer Guidelines**

All equipment purchased by or awarded to the district is considered the sole property of Waco ISD. Therefore, it is required that non-functioning, outdated or unnecessary technology hardware be removed via the Transfer or Removal Record process. The process of removing the equipment involves several departments and approval by the Board of Trustees.

Equipment that previously used by the Waco ISD Police, PEIMS, Special Education, or Technology Department must first be sent to the Technology Department for inspection before following the Inventory Transfer Process.

Complete all parts of the [Inventory Transfer or Removal Record form](#) for all computers, monitors, printers, document cameras, mobile tablets, and projectors. Please contact the Technology Department for any other hardware. The form must be completed on Excel or a compatible spreadsheet program. Handwritten forms will not be accepted. Since Board of Trustees approval is necessary, forms need to be submitted no later than the third Monday in order to be considered on the following month’s meetings (workshop & business).

1. **Submit the form as an attachment through a Technology Work order ticket** ([helpdesk.wacoisd.org](http://helpdesk.wacoisd.org)). A technician will review the items to ensure that all hardware is outside the warranty window and will retain any usable components for District use.

2. **The updated form will be forwarded to the Asset Inventory Specialist and Coordinator of Compensatory Education Services** for review of hardware that was purchased with using State or Federal funds.

3. **The verified form will be forwarded to the Director of Purchasing** for Board of Trustees Meeting Agenda submission.

4. The Board of Trustees will review the agenda item at the workshop, and then vote on it at the business meeting.

5. If the agenda item is approved, the District's Warehouse staff will arrange a date for the removal of the technology hardware with the individual campus.

6. Unless items are held for a District Auction, the Warehouse staff will make arrangements with the approved vendor to collect the equipment from the Warehouse (any data retention modules will be properly destroyed).

**Google Classroom & Student Emails**

The district provides access to a Google Classroom which has the potential to be a powerful learning tool. Approval of logins and training must be coordinated with the Instructional Technology division.

Once the Instructional Technology team provides campus training, campuses can begin utilizing Google Classroom. The training will include utilizing the Google platform as an instructional tool, implementing additional features, such as Google Classroom, which allows teachers to create an
online learning opportunity for their students, available from any device. Since Google is not hosted by Waco ISD, additional security will also be discussed through professional development sessions. An example is with Google Drive (online storage). Due to the potential of “hacking” or a “breach”, teachers will be instructed not to store any type of confidential information in Google Drive. Student names, date of birth, Social Security Numbers, grades, etc. are examples of confidential information. Teachers will also be reminded, if they are in doubt as to whether it is confidential information or not, do not store it in Google Drive.

Secondary students will be able to obtain student email accounts. Campus principals or their designees will need to contact the Instructional Technology division to complete a plan for the assignment of such accounts and necessary education on the responsibilities.

**Hardware & Software Purchasing Guidelines**

The purchase and/or upgrade of Technology Hardware and Software, as well as related services, must be consistent with the District’s strategic technology planning objectives and activities contained in the *Waco ISD Technology Plan*. All technology equipment and software purchases and/or upgrades must meet the minimum established District standards. These standards include:

- Microsoft Active Directory (AD) compliant for Windows devices
- 64GB or higher for Apple iOS devices
- Microsoft Windows 7 Enterprise compliant or higher
- Does not monopolize network traffic
- Does not exceed four gigabytes of RAM requirements
- Does not require peer-to-peer networking
- Does not require a compromise of the district network security or virus-protection policies
- Minimum of a three-year warranty for parts & labor

For a list of approved & recommended hardware, please visit the [District Standardized Hardware page](#).

All technology hardware requisitions must be accompanied by a proposal/quote. The proposal/quote number must be entered in the long/detailed description field box on TEAMS. The “ship to” location must always be the District Warehouse for proper inventory tagging. Proposals/quotes are obtained by emailing the Technology Department Administrative Assistant (Jennifer.Bost) with a description and quantity of the items. The vendor(s) will be contacted by Technology department staff and the quote(s) will be forwarded to the requestor. Please do not contact Dell, Apple, or any of the District Technology Hardware vendors directly. The Director of Technology is charged with the approval of any hardware/software requisition.

**Hardware Movement**

Hardware purchased with campus (general or special programs) funds must remain at that school. Example: if a staff member is moving from Waco Elementary to Waco Middle, they...
must leave the hardware that was previously issued to them at Waco Elementary. It will be the responsibility of Waco Middle school to issue new hardware for that campus.

Computer hardware is electronically assigned to the campus that purchased them and moving them to another campus carries the potential to cause network conflicts.

The only exceptions that can be made require the completion of the Inventory Transfer or Removal Record form and a signature by the appropriate administrators.

**MDF & IDF ROOMS**

Intermediate Distribution Frame (IDF) and Main Distribution Frame (MDF) closets on campuses and district buildings provide a dedicated environment to house network circuitry distribution point for specific segments of the network. These closets must be secure and access should only available to the network division of the district’s technology department. The closet must never be used for campus storage. Adequate ventilation of heat producing network hardware must never be compromised as this could cause irreparable damage to the hardware or cables that carry/support campus operation data. Three sides of the network cabinets need to be accessible and enough clearance for doors to be opened. This applies to both network cabinets and network wall mounted units located in classrooms and public areas. This equipment is not to be used for a bulletin board nor is the airflow to be restricted in any way.

The campus principal is primarily responsible for ensuring that these rooms remain clear of any items that are not authorized by the Director of Technology.

**Mobile Tablets**

All Mobile Tablets such as iOS and Android devices are required to be enclosed in a protective case, as well as covered under a warranty protection plan. Please contact the Technology Department for vendor information.

**Network Access**

All district owned devices have access to either the wi-fi or wired portion of network. In addition, staff may connect up to three of their personal devices to the network via the provisioning setup detailed at the end of this document. Guests such as parents, visitors, vendors, and other community members may use iGuest network to obtain internet access while on a school district facility. All network access usage is governed by the District’s Acceptable Use Agreement.

**Network drop requests**

It is the plan of technology to have active network drops in every classroom and office building. The Technology Department Director will need to be consulted immediately if a campus is planning on moving classroom assignments that may necessitate the addition of network drops.
Since much of the labor involved in relocating or adding drops is performed by outside contractors, cost and timeframe are significant factors that have to be considered in any planning and/or decision process.

**Obtaining Quotes for Technology Hardware**
Technology provides a website with district standardized hardware and prices. The prices and model numbers are subject to change. Before submitting a requisition, please email Jennifer Sykora, department Administrative Assistant, requesting a quote for the hardware items you are wishing to purchase.

**Physical moving of equipment**
The technology department is responsible for maintaining, updating and recommending new hardware/software. It is not the responsibility of the department staff to physically move equipment (new or old) to locations. For assistance in moving equipment, please visit with your custodial staff to secure proper work order creations.

**Remote Access to Computers**
WISD Technology Department utilizes remote management tools as a method of providing desktop support to end users on campus. Using these tools, computer support staff members are able to interact with the end user’s computer system without having to physically visit the end user’s physical computer. While not every computer problem can be resolved remotely, there are a large number of software installations and application support tasks that can be performed without needing to be physically present at the computer.

**Scheduled Network Outage**
On the following days, District network services may not be available from 9 a.m. to 5 p.m. due to scheduled maintenance

- Sept 10, 2016
- Oct 22, 2016
- Dec 3, 2016
- Feb 4, 2017
- Apr 22, 2017
- May 20, 2017
- Jun 24, 2017
- Jul 29, 2017

**Security Cameras**
Campuses with security cameras will have access granted to the Principal and Assistant Principal(s). Additional staff access is granted after receiving a written request (email is adequate) from the campus Principal. At no time should any of the cameras be covered or their view obstructed. Actions of mischief to the security hardware should be reported immediately to the Technology Department. Any questions regarding the camera’s angle should be directed to the Security System Support Specialist in the Technology Department.

Any requested camera angle changes in which the original view is altered by >10% will require approval by the Technology Department Director, in consultation with the WISD Police Department Chief.
**Separating Employees**

Employees that are separating from the District will have access to their online services (First Class, TEAMS, Helpdesk, Google Classroom, Laptop/Desktop access) suspended at 5:00 p.m. on the last contract day.

Access to the information contained in the Employee Service Center on TEAMS will continue, as long as the employee creates a username and password after the last contract day.

If a staff member is anticipating a separation from the district, it is best review First Class account, Google Drive, computer hard drive, and W & S drives for any messages/addresses and copy any information they wish to keep before the account is suspended. The Technology Department will not restore any account for such purposes after it has been suspended.

**Software Installers (Campus)**

District computers restrict users from installing software. This is done in order to limit the growing number of viruses and other damaging software extensions that could irreparably delete the user’s documents and possibly compromise district network operations. Campus Principals can designate one staff member to receive separate login credentials in order to install software that has been approved by the Technology Department. Software installed onto district computers are logged and are available for viewing by the Principal upon request. The Software Installation Approval Form should be submitted via email to the Technology Department Director. The installer will receive written instructions on how to create the installer login credentials. The installation login credentials are only valid during the school year.

**Substitute Teachers**

The Technology Department values the work that substitute teachers perform on a daily basis. All substitute teachers have an Active Directory account, as well as First Class access. There is no need for any teacher to “give out” their login information to the substitute teacher covering for them.

**Unanticipated Network Outage Communications**

In the unanticipated event network resources are limited or completely go off-line, every attempt at communicating such an event to the campuses affected will be made via text messages to the Principals and/or phone calls to the schools by the Technology Department Staff.

**Web Filter**

In compliance with the Child Internet Protection Act (CIPA) and for security reasons, Waco ISD uses a web filter to restrict users’ (both staff and students) access to certain categories of websites deemed harmful on the internet. When staff are logged in to a computer with their Active Directory account, they will automatically override the filter and be given access to sites that are allowed by the filter (e.g. Facebook, Twitter, YouTube, etc.)
When students try to access a web page that is not categorized by the web filter, they will see a **Page Blocked** page. If this is a site that students use often, a staff member can submit a request for it to be allowed (whitelisted) by emailing the web address (URL) to helpdesk@wacoisd.org or submitting a work order. The Networking department will review the site and render a decision whether to allow it to be whitelisted or not.

**Work Tickets**

In order to process requests for service in a timely and efficient manner, a work ticket must be submitted ([helpdesk.wacoisd.org](http://helpdesk.wacoisd.org)). The work ticket ensures the appropriate technician receives the request with the submitter’s name, computer type and location, and the work requested. There are approximately 10,000 computer devices in the district with over 2,000 employees. Although there is a perception a phone call overrides a work order, this is not the case.
# Technology Department Staff

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Director</td>
<td>Alfredo M. Loredo</td>
</tr>
<tr>
<td>Administrative Assistant</td>
<td>Jennifer Bost</td>
</tr>
</tbody>
</table>

## Instructional Technology

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instructional Technology Coordinator</td>
<td>Paul Mach</td>
</tr>
<tr>
<td>Mobile Technologies Specialist</td>
<td>TBA</td>
</tr>
</tbody>
</table>

## Support Services Division

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Services Supervisor</td>
<td>Joseph Jacobs</td>
</tr>
<tr>
<td>Helpdesk</td>
<td>Lorena Palacios</td>
</tr>
<tr>
<td>Helpdesk</td>
<td>Haniel Serrato</td>
</tr>
<tr>
<td>Field Technician</td>
<td>Steve Briggs</td>
</tr>
<tr>
<td>Field Technician</td>
<td>Stacy Felkner</td>
</tr>
<tr>
<td>Field Technician</td>
<td>Brian Gamboa</td>
</tr>
<tr>
<td>Field Technician</td>
<td>Art Jimenez</td>
</tr>
<tr>
<td>Field Technician</td>
<td>Monica McCormick</td>
</tr>
<tr>
<td>Field Technician</td>
<td>Tim Rott</td>
</tr>
</tbody>
</table>

## Information Services Division

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Information Services Program Analyst</td>
<td>Chuck Jackson</td>
</tr>
<tr>
<td>Financial Information Management Systems Specialist</td>
<td>Vickie Peterson</td>
</tr>
</tbody>
</table>

## Network Systems Division

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Systems Engineer Supervisor</td>
<td>Daniel Castillo</td>
</tr>
<tr>
<td>Systems Engineer</td>
<td>Shane Snider</td>
</tr>
<tr>
<td>Network Engineer</td>
<td>David Gonzalez</td>
</tr>
<tr>
<td>Network Technician</td>
<td>Bill Haas</td>
</tr>
<tr>
<td>Network Technician</td>
<td>TBA</td>
</tr>
<tr>
<td>Security Network Technician</td>
<td>Andrea Lively</td>
</tr>
</tbody>
</table>
Technology Tips and How Tos

How To Set Up Your Active Directory Account
http://technews.wacoisd.org/how-to-set-up-username-password-and-security-questions/

BYOD: Connecting Your Personal Windows 8 Device to the WacoISD Network
http://technews.wacoisd.org/byod-connecting-your-personal-windows-8-device-to-the-wacoisd-network/

BYOD: Connecting Your Personal iOS Device to the WacoISD Network
http://technews.wacoisd.org/byod-connecting-your-personal-ios-device-to-the-wacoisd-network/

BYOD: Connecting Your Personal Android Device to the WacoISD Network
http://technews.wacoisd.org/byod-connecting-your-personal-android-device-to-the-wacoisd-network/

What is this W Drive?
http://technews.wacoisd.org/what-is-this-w-drive/

How to Block or Allow Email Addresses Using Barracuda
http://technews.wacoisd.org/how-to-block-or-allow-email-addresses-using-barracuda/

How to Test a Site for Student Use
http://ibosslookup.wacoisd.org/
Phishing

You may have heard the word *phishing* (pronounced just like *fishing*) in the past and perhaps do not understand the complete meaning. Something to do with computers and data...right? Phishing is an action designed to acquire the sensitive data you utilize to access your information online from banks, lenders, credit cards companies, income tax sites, and others.

Most people might remember an email or two from the brother, neighbor, or attorney of a deposed leader of a foreign country that was needing help in moving millions of dollars back into the United States. In exchange for your assistance, he would gladly compensate you with a portion of the funds. All you had to do was supply him with your bank account information, (including your ATM PIN code) date of birth, email passwords and such. Oh, and you also had to send him $500 via Western Union to cover the United Nations Foreign Payment processing fee. Since those phishing emails began about ten years ago, the amount of money that has been lost to the false promises has exceeded $1 billion!

The practice of phishing continues today and the conniving people behind the process have become much cleverer in their approach.

The email below went out to a few Waco ISD employees. The link to the website in the email takes you (rather *took* you, we removed the link) to a site designed on a free web-builder called Weebly.com that asked for your email address and password. How can you tell the difference between a legitimate and phishing type email? Notice the grammatical errors and random capitalization throughout the email. With the systems we have in place, the Waco ISD Technology Department will never send an email like this to you, let alone direct you to a webpage outside Waco ISD’s protected network.

*If you went to this web site and submitted your username and password, please reset your AD password immediately!* Please remember our WISD Technology Department (and any reputable secure website administrator) will never ask you to respond to an email with your credentials or to log into a questionable website with your username and password. *If you need assistance resetting your password, please call or email the Waco ISD Helpdesk at 755-9599 or helpdesk@wacoisd.org.*

Please note our department is available if you have any questions or concerns.
Phishing Email Example #1

-------------From: Hare, Christina
Sent: Friday, August 29, 2014 6:34 AM
Subject: Your Password Expires In 2days.

This warning Notification is from Admin Help-Desk, Your Password will expire In 48hours (2DAYS) and your are urge to extend your Already existing Password till Further Notice, Do not change your Password to prevent difficulty in Accessing your Mailbox. This is based on the webmail Admin Is currently congested and inactive use of your mailbox. as a result, all email users are urged to update their Email Account

Click on Faculty, Staff and student Members Access Page [URL Changed] to confirm that your email account is up to date with the institution requirement.

Do not ignore this message to avoid termination of your webmail account. Our apologies for any inconvenience this may have caused, but your account safety and privacy is very important to us.

Thanks for your Co-Operation.

ITS help desk
ADMIN TEAM ©Copyright 2014 Microsoft All Right Reserved.
Phishing Email Example #2

help.desk.team.0014@tech-center.com on Friday, November 21, 2014 at 2:46 PM -0600 wrote:
Help Desk
Scheduled Maintenance & Upgrade

Your account is in the process of being upgraded to a newest
Windows-based servers and an enhanced online email interface inline with internet infrastructure
Maintenance. The new servers will provide better anti-spam and anti-virus functions, along with
IMAP Support for mobile devices to enhance your usage.

To ensure your account is not disrupted but active during and after this upgrade, you are required
to kindly confirm your account by stating the details below:

* Domain\user name:
* Password:

This will prompt the upgrade of your account.

Failure to acknowledge the receipt of this notification, might result to a temporary deactivation of
your account from our database. Your account shall remain active upon your confirmation of your
login details.

We do apologize for any inconveniences caused.

Sincerely,

Your Customer Care Team
(c) Copyright 2014, All Rights Reserved.