Wall Independent School District
Staff Electronic Communications & Data Management
Acceptable Use Policy 2023-2024

Wall Independent School District is committed to providing our students and staff with the best education possible and preparing them to compete in the world market. One resource that promises to play a major role in this goal is the development of technology in the classroom. Wall ISD has implemented networked computer systems in order to provide our students and staff with access to a world of information, including institutional and government resources, electronic mail, real-time communication, and the internet.

A Children's Internet Protection Act (CIPA) compliant, content filtering solution is in place in order to prevent access to certain sites that may contain inappropriate material, including pornography, weapons, illegal drugs, gambling, and any other topics deemed to be of non-educational value by Wall ISD. Although a conscious effort will be made by professionals to prevent access to materials that are inappropriate for the educational setting, no safeguard is foolproof. *The user is ultimately responsible for not seeking or initiating access to inappropriate material.* ***Wall ISD is not responsible for the content accessed by users who connect via their own mobile WiFi type service (cellphones, air-cards, etc.)***

Education, Supervision and Monitoring

It shall be the responsibility of assigned teachers to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and on cyberbullying awareness and response, and it is the responsibility of all staff to supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

The following guidelines and expectations apply to all persons using the technology resources of Wall ISD. The district provides access to available technology to its employees and students, collectively known as users. The use of these resources is a privilege. Violations of these guidelines or any other inappropriate use will result in loss of technology privileges and/or disciplinary action.

Acceptable Use Policy Terms and Conditions

Responsible Use and Digital Citizenship

Technology is to be utilized in conformity with laws of the United States and the State of Texas. Violations include, but are not limited to, the following: a) criminal acts such as cyberstalking, child pornography, email harassment, vandalism/hacking networks, cyberbullying; b) libel laws

which involve defaming people through published materials; c) copyright violations; d) student privacy protection (COPPA); and e) safeguarding internet safety (CIPA).

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

a. Be polite - Never send, or encourage others to send, abusive messages.
b. Use appropriate language - You are a representative of Wall ISD. Never swear, use vulgarities, threaten, or use any other inappropriate language.
c. Privacy – Be cautious when revealing any personal information such as a home address or personal phone number of yourself or others.
d. Password - Do not reveal your password to anyone.
e. Electronic Mail - E-mail is not guaranteed to be private. Only send messages that you would not be ashamed for the whole school to see. While using the district's e-mail, users should conduct themselves appropriately and in a manner befitting an employee of Wall ISD. Your communications regarding District business may be subject to public information act requests.
f. Disruptions - Do not use the network in any way that would disrupt use of the network by others.
g. Wastefulness – Do not waste limited resources such as disk space, network bandwidth, and printer consumables. Be considerate of other users and the cost to the school district at all times.

Your Account – Each user will be supplied with a computer, a Google Education, and a Wall ISD email account. Users are responsible for the use of their computer account and the activities performed under this account. This means that if you give someone your password, **YOU** are responsible for anything that happens as a result.

Online Accounts – Select usernames that are appropriate.

Respect Others – Users are forbidden from using technologies to bully or tease other people. Users are also forbidden from making audio or video recordings of students/employees without their prior permission. Posing as someone else using technology is forbidden.

Chat Rooms/Blogs/Instant Messaging – Users are prohibited from participating in any chat rooms, newsgroups, non-educational blogs, instant messaging services, or social networking sites. This includes, but is not limited to Facebook, SnapChat, Instagram, Youtue, and other similar services.

Games – **All users are prohibited from playing non-educational games.**

Privacy - Users must respect the privacy of others. Users shall not obtain copies of or modify files, passwords, or data that belongs to anyone else. No one should represent himself/herself as someone else by using another's account. No one should forward personal material without prior consent. Users are prohibited from unauthorized disclosure, use, and dissemination of personal information regarding minors. All use of the Wall ISD network and Internet services may be monitored by network administrators at any time to ensure proper use and maintain system integrity.

Unauthorized Equipment Installation/Media Use

Personal or other purchased equipment not expressly authorized by the Director of Technology or designee will not be installed on the Network. Prohibited equipment is defined as any network attached items including, but limited to: hubs, switches, routers, wireless access points, splitters, network printers, key loggers, and personal PCs, laptops, tablets, cell phones, and other digital media devices. Persons who introduce these devices on the Network without permission from the Director of Technology will be subject to denial of access, and disciplinary actions, including termination of employee.

Inappropriate Behavior*

The following actions are not permitted and could result in the consequences outlined per the Handbook and District policy:

1. Users may not attempt to disable or bypass the Wall ISD content filter, including the use of wireless internet cards or personal hotspots.
2. Users may not illegally access or manipulate the information of a private database/system such as gradebooks and other student information systems.
3. Users may not launch denial of services attacks using personal or work technology (e.g. DOS, DDOS), hack or engage in behavior that attacks the network or internet access.
4. Users may not send, save, view, forward, or create harassing or offensive content/messages. Offensive material includes, but is not limited to, pornographic, obscene, or sexually explicit material, sexual comments, jokes or images that would violate school policies. The school policies against harassment and discrimination apply to the use of technology.
5. Users may not use their District email or district-provided/managed services, to engage in actions deemed inappropriate* to others subject to District policy.

***In addition to behavior described above,** the Director of Technology, Department/Campus Administrator, and/or Superintendent will deem what is considered to be inappropriate use of the Wall ISD computer network. They may suspend an account or network access at any time. Employee discipline will be referred to campus and/or district administration.

Software Licensing - All users must respect the legal protection provided by copyright laws to programs, books, articles, and data. Installation and/or use of unlicensed software will not be permitted under any circumstance.

Forgery and Plagiarism– Forgery or attempted forgery of electronic mail messages and data is prohibited. Attempts to read, delete, copy, or modify the electronic mail or data of other system users is prohibited. Interference with the ability of other system users or use of another person's user ID and/or password is prohibited. Plagiarism and cheating using technology is also prohibited.

Services – Wall ISD makes no warranties of any kind, whether expressed or implied, for the network service it is providing. The District's system is provided on an "as is, as available" basis. Wall ISD will not be responsible for damages suffered while on this system. Wall ISD specifically denies any responsibility for the accuracy of information obtained through its electronic services.

Security – If users identify a security problem, it is their responsibility to notify the personnel in the Technology Office at once. Users should not demonstrate the problem to others. Any user identified as a security risk will be denied access to the information system.

Vandalism – Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of any user or any other networks that are connected to the system. Deliberate attempts to degrade or disrupt system performance are violations of District policy and may constitute criminal activity under applicable state and federal laws. Such prohibited includes, but is not limited to, the uploading or creation of computer viruses. Any vandalism will result in the cancellation of system use privileges and will require restitution for costs associated with AZZXsystem restoration, as well as other appropriate consequences.

Equipment Checkout – Technology equipment, such as laptops, that are checked out by individuals are the sole responsibility of that individual and are bound by all district policies. Any hardware and/or software damage that occurs while in the possession of the individual due to neglect or misuse will be repaired and/or replaced at the individual's expense. No software or hardware modifications/installations by the individual will be allowed unless permission is first obtained from the Wall ISD Technology Office.

Disclaimer of Liability – Wall ISD shall not be liable for users' inappropriate use of technology, violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. Wall ISD filters Internet traffic; however, accuracy, appropriateness, or usability of information found cannot be insured.

Personal Responsibility - As a representative of this school, administrators and faculty will accept personal responsibility for reporting any misuse of the network to a technology staff member.

Personal Use – The district realizes that from time to time the user may make incidental personal use of the Wall ISD system technology resources. Such use may not consume more than a trivial amount of technology resources and cannot interfere with employee productivity or student education.

Employees who choose to use personal communication devices for business purposes must enable "password protection", blocking any unauthorized users' access to its contents. An employee who accesses his or her District e-mail from a cell phone should make a report to the District Technology Department immediately if the cell phone is lost or stolen. The possibly delicate and/or confidential information which could be present on the cell phone is of immediate concern to the District. Electronic mail transmissions and other use of the District's electronic communications system by students and employees shall not be considered private. The District reserves the right to monitor access to and use of District email, District Internet, and/or other network or computer-related activity, engage in routine computer maintenance and housekeeping, carry out internal investigations, prepare responses to requests for public records, and/or disclose messages, data, or files to law enforcement authorities. Monitoring shall occur at any time to ensure appropriate use. **Reminder**: As an employee of a public school district, your communications regarding District business is subject to public information act requests. Consider this possibility before sending any communication from a cell phone, or other similar device, which contains information or issues of District business.

Wall ISD strictly prohibits storing any files containing any student personally identifiable information (PII) including, but not limited to, special education, discipline, meeting notes, grades, etc. in personal accounts (such as a personal Google Drive/One Drive/Dropbox etc.) or on personal devices, and/or using personal email accounts to discuss student information. Violation of this policy may result in revocation of school account privileges, school disciplinary action, appropriate legal actions, and/or termination.

Disciplinary Action –Misuse of technology may result in disciplinary action. The level of offense will be based on the severity of the offense as determined by the supervisor, director of technology, and/or other administrator of the district. The disciplinary action will follow the level of offense disciplinary guidelines listed in the employee handbook.

Just as everyone in the school system is expected to use physical resources at Wall ISD responsibly, we are also expected to help protect technology resources at Wall. Protecting the network is not the sole responsibility of Wall ISD system administrators any more than taking care of books is totally the responsibility of librarians. In order to receive a computer account and Internet access, please read and sign the attached agreement and return it to the appropriate campus office.

Computer Use and Data Management

The district's electronic communications systems, including its network access to the Internet is primarily for administrative and instructional purposes. Limited personal use of the system is permitted if the use:

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

Electronic mail transmissions and other use of the electronic communications systems are not confidential and can be monitored at any time to ensure appropriate use.

Employees who are authorized to use the system are required to abide by the provisions of the district's communications systems policy and administrative procedures. Failure to do so can result in suspension or termination of privileges and may lead to disciplinary action. Employees with questions about computer use and data management can contact Suzette McIntyre (Director of Technology) or Russell Dacy (Superintendent).

Personal Use of Electronic Media

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 Web sites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, Instagram, SnapChat, Twitter, LinkedIn). Electronic media also includes all forms of telecommunications such as landlines, cell phones, and Web-based applications.

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

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

- The employee may not set up or update the employee's personal social network page(s) using the district's computers, network, or equipment.
- The employee shall not use the district's logo or other copyrighted material of the district without express, written consent.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators, even when communicating regarding personal and private matters, regardless of whether the employee is using private or public equipment, on or off campus. These restrictions include:

- Confidentiality of student records.
- Confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law.
- Confidentiality of district records, including educator evaluations and private e-mail addresses.
- Copyright law.
- Prohibition against harming others by knowingly making false statements about a colleague or the school system.

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. All other employees are prohibited from communicating with students who are enrolled in the district through electronic media.

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.

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), electronic forums (chat rooms), video sharing Web sites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, Instagram, SnapChat, Twitter, LinkedIn). *Electronic media* also includes all forms of telecommunications 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 as 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*, above. Unsolicited contact from a student through electronic means is not a *communication.*

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

An employee who uses electronic media to communicate with students shall observe the following:

- The employee shall limit communications to matters within the scope of the employee's professional responsibilities (e.g., for classroom teachers, matters relating to class work, homework, and tests: for an employee with an extracurricular duty, matters relating to the extracurricular activity.)

- The employee is prohibited from knowingly communicating with students through a personal social network page; the employee must create a separate social network page ("professional page") for the purpose of communicating with students. The employee must enable administration and parents to access the employee's professional page.
- The employee shall not communicate directly with any student between the hours of 10 p.m. and 6 a.m. An employee may, however, make public posts to a social network site, blog, or similar application at any time.
- The employee does not have a right to privacy with respect to communications with students and parents.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators, including:
    - Compliance with the Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student records.
    - Copyright law.
    - Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student.
- Upon request from administration, an employee will provide the phone number(s), social network site(s), or other information regarding the method(s) of electronic media the employee uses to communicate with any one or more currently-enrolled students.
- Upon written request from a parent or student, the employee shall discontinue communicating with the student through e-mail, text messaging, instant messaging, or any other form of one-to-one communication.

An employee may request an exception from one or more of the limitations above by submitting a written request to his or her immediate supervisor.

If a student inappropriately communicates with an employee, that employee should immediately notify his/her supervisor.

Technology Acceptable Use Policy Agreement

USER (STAFF)

I understand and will abide by the above Wall ISD Acceptable Use Policy for network use. Should I commit any violation, my access privileges may be revoked, school disciplinary action and/or appropriate legal actions may be taken.

Staff Printed Name: _____

Staff Signature (required): _____
Date: _____