Waco Independent School District

Acceptable Use Agreement

Please read the following information carefully.
This is a legally binding document of Waco Independent School District.

I. OVERVIEW

The Waco Independent School District (WISD) owns and maintains a computer system/network (WISD Network – further defined below). WISD permits students and employees (herein referred to as WISD User(s)) to use and access the WISD Network pursuant to Board Policy [DH (Local), CQ (Local)] and this Agreement. WISD’s goal is to promote educational excellence by providing a safe, ethical, and productive electronic learning environment to support effective, meaningful classroom instruction and administrative needs. This document is intended to outline the responsibilities of acceptable use while utilizing the WISD network or systems. It will be the WISD Users responsibility to follow the rules for appropriate and acceptable use.

Definition of WISD Network: WISD’s Network includes all of its computer systems, electronic communication systems and networks of any configuration of hardware and software, including but not limited to the following:

- District provided telephones, and mobile technologies
- Email communication, and other collaboration systems and platforms
- 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 (Cloud or District server based);
- District-provided Internet access
- District-filtered public Wi-Fi
- Virtual environments
- New technologies as they become available

Definition of a system account: Any login and password information disseminated to WISD Users for the purpose of educational or administrative duties, whether cloud or district hosted. A system account includes, but is not limited to: Active Directory (AD), Eduphoria, TEAMS, Milestone Camera systems, login to a non-/domain WISD computer, ID camera software, or accounts established to manage online learning programs (such as, but not limited to, SmartyAnts, Achieve3000, iStation, and others).

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

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

In addition, access to the WISD Network is a privilege, not a right. The smooth operation of the WISD Network relies upon the proper conduct of the WISD Users who must adhere to this Agreement. The matters addressed and set forth in this document are so that WISD Users are aware of the responsibility to follow the rules for appropriate and acceptable access and use. In general, this requires efficient, ethical, and legal utilization of the network and system resources. Noncompliance may result in suspension of access or termination of privileges along with other appropriate disciplinary action consistent with WISD 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 WISD Policies. All WISD Users must abide by ethical standards when communicating with other WISD Users, regardless of whether such communication takes place on campus, during instructional time, through use of the WISD Network or not. Violations of District Policy or applicable laws may result in criminal prosecution as well as disciplinary action by WISD.

**Definition of a WISD Administrator** – a WISD Administrator is defined as a campus principal or Superintendent's Cabinet.

**II. PHILOSOPHY**

a. **Risk** – Even with filtering, firewalls, 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 WISD Users may access material that may not be of educational value in the school setting.

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

c. **WISD Administrator Responsibility** – Upon being notified, it is the campus administrator’s responsibility to contact the appropriate technology personnel by contacting the Technology Help Desk so the material in question can be reviewed.

**III. TERMS AND CONDITIONS**

**Responsible Use:** WISD Network access may be used to improve learning and teaching consistent with the educational goals of WISD. WISD expects legal, ethical, and efficient use of the WISD Network. WISD approved email accounts will be provided for WISD Users based on WISD initiatives. WISD approved social media activities that are educationally related may be used. At no time should personal use of the WISD Network come in conflict or hinder a WISD User’s expected responsibilities.

a. **Privilege:** Use of a personal WISD Network account is a privilege, not a right.

b. **Limited Personal Use:** is permitted as long as it (1) does not impose any tangible cost to WISD, (2) does not unduly burden WISD’s technology resources, and (3) has no adverse effect on an employee’s job performance or on a student’s academic performance. WISD will provide a
filtered, wireless public network to which staff and students will be able to connect personal computer devices, including, but not limited to, cell phones, tablets and laptops for instructional and administrative functions. These personal devices are the sole responsibility of the owner. WISD assumes no responsibility for personal computer devices, including, but not limited to a device being lost, loaned, damaged or stolen. Accordingly, limited WISD time or resources will be spent trying to locate stolen or lost personal computer devices. Each WISD User is responsible for his/her personal device(s), including, but not limited to set up, maintenance, charging and security. WISD staff will not diagnose, repair or install software on a WISD User’s personal computer device. Should (1) prohibited, unacceptable and/or inappropriate use/access and/or (2) a security breach of the WISD Network that involves (or potentially involves) a WISD User’s personal computer device occur, be detected and/or suspected, appropriate WISD staff may search, examine, access, and/or inspect the WISD User’s personal device(s) in accordance with applicable laws in order to confirm or rule out any prohibited, unacceptable and/or inappropriate use/access and/or security breach involving the WISD Network.

c. **Subject to System Administration:** All WISD Network accounts and computer usage are subject to inspection by the WISD Network system administrators for virus scanning, monitoring for inappropriate use, and investigation of suspected misuse at the authorized direction of WISD Administration. No WISD computer, network, or internet usage (including usage by a personal electronic device) shall be considered confidential.

Accordingly, WISD Users should not use the WISD Network to send, receive or store any information, including any kind of electronic messages (email, text etc.) the WISD User considers personal or confidential and wishes to keep private. WISD reserves the right to access, review, copy, modify, delete or disclose such files for any purpose. WISD Users should treat the WISD Network like a shared or common file system with the expectation that all information and electronic files sent, received, or stored anywhere in the WISD Network system is subject to inspection, and will be available for review by any authorized representative of WISD for any purpose.

d. **Required Training:** In addition to adhering to the WISD Acceptable Use Agreement, all WISD Users will complete annual training for appropriate technology use, as required by WISD.

**IV. PROHIBITED, UNACCEPTABLE AND/OR INAPPROPRIATE USE:** Prohibited, unacceptable and/or inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations by WISD, that violate the rules of network etiquette, or that interfere with, hamper or harm the integrity or security of the WISD Network, as well as the following:

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 the WISD Network may result in litigation against the offender by the proper authorities. If such an event should occur, WISD 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. This includes any use of district-owned devices
for personal for-profit business or gain, unless district-approved or affiliated.

c. Vandalism/Mischief: Vandalism and mischief are prohibited. Vandalism is defined as any malicious attempt to harm or destroy data or devices of another WISD 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 WISD 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 WISD 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 and such activities as solicitation, fundraising, or religious activities is prohibited.

e. File/Data Violations: Deleting, examining, copying, or modifying files and/or data belonging to other WISD Users is prohibited. Posting, sharing or storing personally identifiable information (PII) including, but not limited to, medical information, student accommodations (IEP, ARD, 504, etc.), social security numbers, phone numbers, addresses, etc., to a third-party cloud platform (e.g. GSuite) is prohibited.

f. System Interference/Alterations/Hacking: Attempts to exceed, evade or change resource quotas are prohibited. Installing unauthorized network access points or other connections, causing or attempting to cause network problems, including but not limited to, network congestion through mass consumption of system resources, attempts to disable the WISD Network filter or compromising the integrity of the firewall, and unauthorized access (hacking) into any part of the WISD Network are prohibited.

g. Inappropriate Speech/Messages: The following restrictions against inappropriate speech and messages apply to all communication sent and/or accessed through the WISD Network, including all e-mails, instant messages, texts, web pages, blogs, wikis, or other avenues of electronic communication. WISD Users shall not send obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful messages. WISD Users shall not post information that could cause damage, danger, or disruptions, or engage in personal attacks, including prejudicial or discriminatory attacks. WISD 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 is prohibited. 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 WISD User’s home and personal electronic communication use (outside of the WISD Network) can have an impact on WISD and its schools, students and/or staff. A WISD User’s personal electronic communication expression including, but not limited to, threatening messages, a violent or sexual website, a text, or a post that creates a likelihood of disruption of the school/district’s operation may result in WISD disciplinary action and/or criminal penalties.
i. **Bullying/Harassment:** WISD takes cyber bullying and harassment by electronic communication very seriously, and it will not be tolerated. WISD Users shall not use the WISD Network to intimidate, threaten, bully, harass, or embarrass students or WISD Users. WISD Users who engage in such activity on school grounds or who engage in such activity off campus and create a disruption of school operations (or the reasonable potential exists) shall be subject to disciplinary actions as well as possible criminal penalties.

j. **Sharing Credentials:** Do not use your login for another individual’s use of a system. When a WISD User logs into a system, that user must remain the operator of that system for the entirety of that session. Each user is assigned a specific set of credentials for their own use. Sharing of assigned credentials is strictly prohibited, unless explicitly allowed by an authorized district administrator.

V. **SECURITY:** Security of the WISD Network is a high priority.

a. **Reporting Security Problems:** If a WISD User identifies or has knowledge of a potential security problem on the WISD Network, the WISD User must notify a teacher, campus principal, system administrator, and/or the Superintendent’s designee. The WISD User shall not reveal or demonstrate the problem to others.

b. **Impersonation:** Attempts to login to, or use of an already logged in session, to the WISD Network as a system administrator or as another WISD User may result in suspension of access to the WISD Network, as well as other appropriate disciplinary or legal action in accordance with the Student Code of Conduct, Board Policy, or applicable laws.

c. **Password Management:** Saving passwords to your browser is dangerous. Do not write your passwords down, share them with anyone or let anyone see you log into devices or websites.

d. **Security Risks Denied Access:** Any WISD 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 WISD Network and all electronic devices in a manner that is appropriate to the student’s age and the circumstances of use.

f. **Filtering Services:** WISD Users may not disable or bypass the WISD Network filtering service at any time. Authorized staff may temporarily or permanently unblock access to sites containing appropriate material if the filtering service has blocked access to such sites.

g. **Bandwidth:** Bandwidth utilization is monitored. WISD 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, WISD Users may not:

   i. Download software or files that are not for educational purposes;
   ii. Play online games that have not been approved by the district;
   iii. View non-curriculum based streaming videos/movies; or
   iv. Set their Internet browser home page to a digital media rich site (i.e. CNN, Yahoo, MSN).
VI. INTERNET SAFETY: Internet safety of WISD Users in their use of the WISD Network is a high priority.

- **a. NEVER** give your username/password to anyone.
- **b. NEVER** tell anyone any district personnel information. Beware of social engineering. This includes, but is not limited to, 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.
- **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.
- **g. A WISD User who becomes aware of prohibited, unacceptable and/or inappropriate use (defined above) should not respond; instead, a teacher or administrator should be notified immediately.**

VII. CONSEQUENCES OF VIOLATION: Any attempt to violate the provisions of this Agreement will result in revocation of the WISD User’s account, regardless of the success or failure of the attempt. Student users may face WISD disciplinary action (Student Code of Conduct) and/or appropriate legal action. Staff users may face WISD disciplinary action up to and including employment termination and/or appropriate legal action. In the event of a claim that a user has violated these guidelines, WISD will provide the user with due process in accordance with the Student Code of Conduct, Employee Handbook, and District policies and procedures.

- **a. Final Determination:** The Superintendent or the designee will make the final determination as to what constitutes prohibited, unacceptable and/or inappropriate use.

- **b. Denial, Revocation, or Suspension of Accounts:** The superintendent/designee, departmental director, campus principal, and/or the system administrator in accordance with WISD disciplinary procedures may deny, revoke, place restrictions, or suspend an account.

DISCLAIMER

WISD makes no warranties of any kind, whether expressed or implied, regarding or in connection with the WISD Network or any WISD User’s use or access thereto. WISD is not responsible for any damages claimed and/or suffered by any WISD User from any use and/or access (or lack thereof) to the WISD Network. 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. WISD is not responsible for phone/credit card bills or any other charges incurred by WISD User. Use of any information obtained via the WISD Network is at the WISD User’s own risk.

WISD is not liable for any individual’s prohibited, unacceptable and/or inappropriate use of the WISD Network including, but not limited to, electronic communication systems or violations of copyright restrictions or other laws or for costs incurred by WISD Users through use of the WISD Network. WISD shall not be responsible for ensuring the availability of the WISD Network or the accuracy, age appropriateness, or usability of any information found on the Internet.
Acceptable Use Agreement Acknowledgement Form

I understand that my access to and use of the WISD Network including, but not limited to, text messaging and social media with WISD provided resources/devices, is not private and may be viewed by WISD officials. Any third party accounts that I use for educational purposes, must also adhere to this Acceptable Use Agreement. I understand that WISD will monitor my activity on the WISD Network.

I have read the WISD Acceptable Use Agreement and agree to abide by its provisions. In consideration for the privilege of using the WISD Network and in consideration for having access to the public networks, I hereby release WISD, its trustees, directors, officers, agents, employees, and any institutions with which they are affiliated, from any and all claims and damages of any nature arising from my access to, use of, or inability to access/use the WISD Network including, without limitation, the type of damages identified in the Agreement, Board Policy, and/or any administrative regulations.

For WISD employees: WISD employees will acknowledge consent to and execution of this Agreement by their signature below, confirmed receipt of the Waco Independent School District Employee Handbook, or consent of the login disclaimer on WISD Active Directory and wireless network systems.

For WISD students/parents: WISD students/parents participating in the online registration process will acknowledge consent to and execution of this Agreement document as part of the registration process. WISD students/parents not participating in the online registration process will acknowledge consent to and execution of this Agreement by signing a hard copy as part of the campus registration process.

Printed Name _____________________________________________________________

Campus ___________________________________________________________________

Employee/Student ID: ___________________________________________________________________

Signature _________________________________________________________________________

Date __________________________________________________________________________