District Technology Acceptable Use Policy

Acceptable use of District Technology occurs where the primary purpose of such use is to improve student learning and prepare students to be career ready graduates.

By using District technology and networks, Learners implicitly agree to the terms of this Acceptable Use Policy. If a Learner is uncertain about whether a particular use is acceptable, he or she should consult a teacher, administrator or other appropriate District personnel.

Based on the notice provided by the PARENT/GUARDIAN/STUDENT NOTIFICATION & INFORMATION HANDBOOK, District Technology policies and regulations (e.g., 0440.1, 6163.4), and students participation in District Technology, this is to highlight that parents, guardians, and students assent to the Acceptable Use Policy and agree not to hold the District or any District staff responsible for the failure of any District Technology protection measures, violations of any legal restrictions, or user mistakes or negligence. Further, by virtue of this notice, assent is also given to indemnify and hold harmless the District and District personnel for any damages or costs arising from or related to use of District Technology and/or any violation of the Acceptable Use Policy.

SUMMARY*: This Acceptable Use Policy ("AUP") was written to inform students, their families, and District staff about acceptable ways in which Fresno Unified School District ("District") information technology may be used. The District's information technology and systems will be referred to as "District Technology" in the rest of this document.*

District Technology Responsible Use

I am responsible for practicing positive digital citizenship and ethical conduct.

- I will practice appropriate behavior and contributions on websites, social media, discussion boards, media sharing sites, and all other electronic communications, including new technology.
- I will be honest in all digital communication.
- I understand that what I do and post online must not disrupt school activities or compromise school safety and security.
- I will use school appropriate language in all electronic communications, including email, social media posts, audio recordings, video conferencing, and artistic works.
- I will not send and/or distribute hateful, discriminatory, or harassing digital communications, or engage in sexting.
- I understand that bullying in any form, including cyberbullying, is unacceptable.

- I will not seek out, display, or circulate material that is hate speech, sexually explicit, or violent.
- I will not share personal information about myself or others including, but not limited to, names, home addresses, telephone numbers, birth dates, or visuals such as pictures, videos, and drawings for non-educational purposes or non-District business.
- I will not post pictures, student work, or other items that are in violation of FERPA*.
- I understand that the use of the District technology for illegal, political, or commercial purposes is strictly forbidden.

I am responsible for the use and care of my computer.

- I will bring my computer every day to school, charged and ready for learning.
- I will ensure the computer is secure and safe.
- I will discuss with my parents or guardian expectations regarding the use of the Internet and the device.
- I will not alter, deface, or remove any district labels on my computer.
- I will return borrowed devices in the same condition as it was given to me.

I am responsible for my passwords and my actions on District technology.

- I will not share any school or District usernames and passwords with anyone.
- I will not access the account information of others.
- I will log out of unattended equipment and accounts in order to maintain privacy and security.
- I understand devices issued to students and staff are for learning or District business.

I am responsible for respecting the works of others.

- I will follow all copyright (http://copyright.gov/title17/) guidelines.
- I will not download illegally obtained music, software, apps, and other works.

*****Family Education Rights and Privacy Act (FERPA) is a federal law that requires confidentiality of student information. Publicly posting students personal information, student records or graded work is a violation of FERPA. To learn more about FERPA beyond responsible use and posting online please visit https://studentprivacy.ed.gov/.

Definitions*:* As used in this document, the word "Learner" includes anyone—employees, students, parents, vendors, and guests—who uses District Technology. Only Learners who agree to this Acceptable Use Policy are authorized to use District Technology.

The use of District Technology is offered to students for educational purposes, as a privilege that must be safeguarded by all learners. The District is committed to improving student achievement and preparing all students to be career ready graduates, and uses District Technology for this purpose. District Technology is issued to appropriate staff to perform their

job duties.

District Technology includes, but is not limited to, cell phones, computer hardware, laptops, classroom display panels, document cameras, tablets, e-readers, software (including cloud resources), hotspots, local wired and wireless networks, and access to the internet. These items provide tools that can be used to access information and communicate with people, enhance learning, and enable the district to operate efficiently. Technology and people's use of technology is always changing so it is critical that the District ensure a safe learning environment for students and staff; safeguards for the privacy of electronic data; and protect the District's technology assets. District Technology remains at all times the property of the District.

Technology Acceptable Use

This Acceptable Use Policy shall conform to existing district policies including Board Policy 0440 and 0440.1 (Technology Board Policies & Administrative Regulations), as well as established procedures and copyright laws. If any portion of these policies conflicts with federal, state or local laws, those laws take precedence, leaving the remaining policies in this AUP in full effect.

This Technology AUP is intended to:

- Prevent or discourage unauthorized access and other unlawful activities online;
- Prevent or discourage unauthorized disclosure of or access to sensitive information;
- Comply with the Children's Internet Protection Act of 1997 ("CIPA");
- Define policies for managing electronic documents that are the property of the District.
- Enhance teaching and learning;
- Increase safety for students and staff;
- Improve the efficiency of district technology systems;
- Ensure alignment with the District's Core Beliefs and Commitments;
- Ensure compliance with applicable district policies, state and federal laws; and
- Educate students, staff, and others who use the District's technology

Filtering. The District will use a variety of technology protection measures on the District's networks to block or filter, to the extent practicable, access to visual depictions that are obscene, pornographic, or harmful to minors, or other content that is not academically relevant. Filtering measures are installed on district devices to protect the user and the device that operate away from the District network. Learners should have no expectation of privacy regarding their use of District property, network, and/or Internet access or files, including email or other forms of communication using District Technology. While our intent is to make computer access available to students to support their educational growth, students may find ways to access inappropriate material as well. Ultimately, parents and guardians are responsible for setting and conveying the standards that their students should follow when

using technology. Disabling content filtering technologies on District issued devices or using tools to circumvent the content filter is a violation of this policy.

Distance Learning and Remote Workers. I understand that I am bound by the Acceptable Use Policy (AUP) regardless of my physical location. I also recognize that FUSD has limited ability to assist in network-related issues. The District may request reimbursement for lost, stolen, or damaged equipment if negligent. Upon request, users are required to bring their District issued device occasionally for a check-up, re-imaging, or support.

Staff Issued and One to One Computers. Laptops and computers issued to students and staff remain the property of the District. I understand that I am responsible for keeping the device safe and only used for their intended purpose while it is in my care. The District may remotely maintain the device by installing software, updating software, or installing security patches.

Bring your Own Device ("BYOD"). Some Learners may choose to bring their own technology. BYOD devices must meet or exceed the minimum specifications established by the District for effective learning. Check the Fresno Unified website for current minimum specifications. If Learners do bring their own devices, they are still subject to this AUP to the extent that their device uses District Services and Networks (wired or wireless) to access internal or internet-based information and data. Internet access from BYOD devices will be content filtered while on the District network. The District does not content filter BYOD devices while away from the District network. Students and parents should be aware that devices are subject to search by school administrators if the device is suspected of a violation of the student misconduct. If the device is locked or password-protected, the student will be asked to unlock the device at the request of a school administrator. The District is not responsible for damage or harm to persons, files, data, hardware, or service interruptions while students are using their device. The property owner assumes any risk or loss by bringing their device.

Digital Classroom Management. As part of our commitment to providing a safe and conducive learning environment, the district utilizes classroom management software to support teachers in managing classrooms effectively. The classroom management software is utilized exclusively during in-person classes and on district-issued computers connected to the school district's network. This system allows for the viewing of student screens on school-issued devices, content sharing, and classroom settings management. Students are expected to adhere to the guidelines outlined in the technology acceptable use policy, which includes the responsible use of the classroom management software. For questions or concerns, please contact your teacher or school administrator.

Lost or stolen devices. A police report will be filed for lost or stolen devices and the device will be remotely locked if possible. Staff is responsible for reporting lost or stolen devices immediately to Risk Management. Parents report lost or stolen devices to the parent and student help desk.

Obligations. Learners and other users are required to follow this policy and report any misuse of District Technology, including the District's network or the internet to a supervisor or other appropriate District personnel. Access to District Technology is provided primarily for education and District business. Staff may use the internet for incidental personal use during duty-free time.

Violations. Violation of these policies may result in one or more of the following: disciplinary action and/or termination for employees and temporary staff; termination of contracts for consultants or contract employees; reimbursement to the District for disallowed charges; or dismissal for interns and volunteers. In the case of a student violation, the violation can result in disciplinary action as deemed appropriate by site administration up to and including removal of technology privileges, removal from class, suspension and expulsion. Additionally, individuals are subject to loss of access privileges, civil, and if warranted, criminal prosecution. The District will attempt to tailor any disciplinary action to the specific issues related to each violation.

Unacceptable Uses of District Technology

Listed below are several examples of inappropriate activities using District Technology. The list is not meant to be all-inclusive but is representative of inappropriate uses. The District reserves the right to take immediate action regarding inappropriate activities that (1) create security and/or safety issues for the District, students, employees, schools, network or computer resources; (2) expend District resources on content that the District in its sole discretion determines lacks legitimate educational content/purpose; or (3) are otherwise determined by District as inappropriate.

Inappropriate activities include:

1. Violating any state or federal law or municipal ordinance, such as, accessing or transmitting pornography; obscene depictions; materials harmful to minors; materials that encourage others to violate the law; confidential information; or copyrighted materials.
2. Criminal activities that can be punishable under the law.
3. Selling or purchasing illegal items or substances.
4. Obtaining and/or using anonymous email or "anonymizer" sites, especially for the purpose of evading the district's content filtering systems; spamming email accounts; spreading viruses; or conducting phishing attacks.
5. Causing harm to others or damage to their property.
6. Using profane, abusive, or impolite language; cyberbullying, including threatening, harassing, or making damaging or false statements about others; or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.
7. Deleting, copying, modifying, or forging other user's names, emails, files, or data disguising one's identity, impersonating other users, or sending anonymous email.

8. Damaging technology, equipment, files, data, or the network in any way, including intentionally accessing, transmitting, or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance.
9. Using any District Technology to pursue “hacking”, whether on targets internal or external to the district or attempting to access information protected by privacy laws.
10. Accessing, transmitting, or downloading large files – in particular, but not limited to, using “torrent” software to illegally download copyrighted digital materials – or using valuable bandwidth for non-academic activities such as network games or serving as a host for such activities.
11. Using email or web services to distribute “chain letters” or any type of “pyramid schemes”.
12. Using web sites, email , networks, or other technology for political uses or personal gain, including advertising, or promoting non-district websites or commercial efforts and events. District internet and intranet property must not be used for personal benefit. Learners must not intentionally access, create, store, or transmit material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or material that harasses, insults or attacks others. Learners must not violate any applicable copyright laws. That includes but is not limited to, the installation of software on district computers for which software the Learner does not have a valid and unexpired software license.

Supporting Information or Additional Obligations

The following information or additional obligations support the District Technology AUP.

Network Security and Password Policies

1. Learners must report any weaknesses in the District’s Internet and intranet security or any incidents of possible misuse or violation of this agreement to the District Webmaster, by sending email to:webmaster@fresnounified.org.
2. Learners must not attempt to access any data or programs for which they do not have authorization or explicit consent.
3. District Technology includes networks and services that are shared resources. Learners must not purposefully engage in activities that deliberately degrade the performance of District Technology systems and related Information Technology property; deprive an authorized District Learner access to a District resource; obtain extra resources beyond those allocated; or circumvent the District’s security measures.
4. Learners must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of the District’s Information Technology systems and related Information Technology property.
5. All private data must be kept confidential and secure by the Learner. The fact that the data may be stored electronically does not change the requirement to keep information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. If this data is stored in a paper or electronic format, or if the data is copied, printed, or

transmitted electronically the data must still be protected if it is confidential and secured.

6. All software programs, applications, source code, object code, documentation and data shall be guarded and protected.
7. The District reserves the right to remove any content (organizational or personal) on the internet or intranet at any time, without cause or notice.
8. There is no guarantee of personal privacy or access to the District's Technology. The district reserves the right to search and/or monitor any information created, accessed, sent, received, and/or stored in any format by any district employee on district equipment or any equipment connected to the district's network.
9. All commercial software used on District Technology systems are copyrighted and designated for District use. Learners must abide by all license agreements.

Artificial Intelligence

The use of Artificial Intelligence (AI) technology in our educational environment is intended to enhance learning experiences and foster innovation. Artificial Intelligence (AI) technology is defined as and includes, but is not limited to, Large Language Models (LLM), Machine Learning (ML), and Natural Language Processing (NLP) Platforms. All learners are expected to utilize AI resources responsibly and ethically. This includes respecting the privacy of individuals, being mindful of the accuracy and reliability of AI-generated information, and refraining from using AI for malicious or inappropriate purposes.

1. Learners will follow all guidelines set by teachers and school site staff regarding the use of AI as part of planning, instruction, and learning.
2. Learners must abide by the AI platform's terms of service (TOS) and federal and state student data privacy laws, and teachers and staff must solicit parental consent when necessary.
3. Learners are prohibited from using any AI system to access, create, or display harmful, deceptive, or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit or that could be construed as harassment or disparagement of others based on their sex, or perceived race, color, ancestry, national origin, age, religious creed, marital status, pregnancy, physical or mental disability, medical condition, genetic information, military and veteran status, sex, sexual orientation, gender, gender identity, or association with a person or group with one or more of these actual or perceived characteristics or interact with the AI in a manner that supports any of the above.
4. Learners shall not share confidential information or personally identifiable information with an AI system of themselves, students, staff members, or others. Personally identifiable information includes, but is not limited to, a person's name, address, email address, telephone number, Social Security number, or other personally identifiable information.
5. Learners will not employ AI systems to make high-stakes decisions that significantly impact people's lives without proper human oversight, transparency, or the ability to appeal.

6. Learners will not allow AI systems to run unchecked and make decisions that could jeopardize safety in dangerous industrial settings, vehicles, infrastructure, etc.

Password Policy

1. Passwords should be treated as confidential information.
2. No personnel should ask, or be given , another Learner password, even for support purposes.
3. Password should be changed at least every 180 days. However, the district may, at its sole discretion, enforce periodic password changes based on role responsibility and usage.
4. Default passwords should be changed within one day.
5. Password complexity must conform to the password policy based on the user's role, responsibility, usage, or appropriateness for the learner's age.
6. Passwords must not include your employee number, name, SSN, phone number, birthday, or the name or your department or school.
7. All security violations shall be reported to the school or department administration.

Access Controls, Information Security, and Accountability

1. Departments and schools that have District Technology must provide appropriate access controls in order to monitor and protect business data and associated programs from misuse.
2. All Learners are responsible for managing their own use of District Technology and are accountable for their actions relating to security. Learners are also responsible for reporting any suspected or confirmed violations of this policy to the appropriate management responsible for FUSD Information Technology system security incident handling.
3. Periodic user cybersecurity assessments may be conducted to measure organizational preparedness or to support staff in cyber-safety education.
4. Access to FUSD Information Technology equipment must be properly documented, authorized and controlled.
5. Access authority for each Learner will be reviewed on a regular basis, as well at each job status change such as: a transfer, promotion, demotion, or termination of service.
6. Schools and Departments responsible for the custody and operation of District technology shall be responsible for proper authorization and related technology use, the establishment of effective use, and reporting of performance to management.
7. Some District staff are required to use a VPN or other approved network security procedures to access internal systems or data when working remotely.
8. On termination of the relationship with FUSD all security policies for FUSD apply and remain in force surviving the terminated relationship.
9. Staff accessing district resources may be required to use Multi-Factor Authentication (MFA).
10. Staff will be required to use elevated access logins when accessing sensitive

district resources to ensure limited and controlled access within the organization's enterprise technology ecosystem.

11. Misuse of non-human accounts, which are user accounts created for automated or programmatic access to systems and services, is strictly prohibited. This includes unauthorized access, manipulation, or the development of automated bots, processes, or scripts by employees to carry out unauthorized activities.
12. Access to district online resources may be blocked from locations outside of the United States.

Document Retention

It is each employee's responsibility to save and/or archive email that he or she receives and wishes thereafter to access, or that are District records and required to be retained by law. Emails must be kept in your online email inbox or archive folder only, or in an appropriate SharePoint or OneDrive Document Repository. Archiving district-related emails outside a Fresno Unified system is prohibited.

If you store such documents outside of their required locations, you may be subject to disciplinary actions.

Incidental Use

As a convenience to the District Learner community, incidental personal use of District technology is permitted. The AUP Policy still applies to incidental use with the addition of the following limitations:

1. Incidental personal use of District technology by Learners does not extend to family members or other acquaintances.
2. Incidental personal use must not result in direct costs to the District.
3. Incidental personal use must not interfere with the normal performance of an employee's work duties or student learning.

Compliance / Regulation Contributed to by this Policy

This Acceptable Use Policy relies, in part, in requirements or concept from the following:

1. Family Education Rights and Privacy Act 1974 (FERPA)
2. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
3. Children's Internet Protection Act of 2000 (CIPA)
4. Protection of Pupil Rights Amendment (PPRA)
5. Copyright Act of 1976
6. Foreign Corrupt Practices Act of 1977
7. Computer Fraud and Abuse Act of 1986
8. Computer Security Act of 1987
9. California Ed Code

10. Student Online Personal Information Protection Act (SB1177)

Acceptance

Based on this notice and your student's use of District Technology, parents and students assent to this Acceptable Use Policy and acknowledge the importance of personal responsibility to these policies including, but not limited, to the following.

Parent/Guardian Responsibilities:

- Supervise your student's use of the device outside of the District network.
- Review and discuss the District's Acceptable Use Policy (AUP) with your student.
- Return the device if requested, or your student withdraws or graduates from Fresno Unified.
- Pay fees associated with replacement or repair of damaged computers.
- Indemnify and hold harmless the District and District personnel for any damages or costs arising from or related to a violation of the Acceptable Use Policy.