



Fresno Unified School District

Technology Acceptable Use Policy

SUMMARY: *This policy was written to inform students, their families, and staff about the acceptable ways in which information technology systems may be used in Fresno Unified School District. Fresno Unified School District is committed to improving student achievement and preparing all students to be career ready graduates. District Technology, which includes but is not limited to: computer hardware, software, and the Internet provide powerful tools to access information and communicate with people, enhancing learning and enabling the district to operate. With the constant introduction of new technology, new ways to communicate, and new ways to access and transfer information, it is therefore critical that the district continue to define a policy that ensures a safe learning environment for students and staff as well as the protection of the district's technology. The use of FUSD technology is offered to students and staff as a privilege which must be safeguarded by all learners.*

Technology Acceptable Use Policy

The Fresno Unified School District (FUSD) provides technology, including, but not limited to: computers, networks and Internet services. **Acceptable use of FUSD technology is for the purpose of improving student learning and to prepare students to be career ready graduates.** FUSD technology remains at all times the property of FUSD.

This policy shall conform to district policies including Board Policy 0440 (Technology Board Policy & Administrative Regulations), established procedures and copyright laws, and shall not violate federal, state or local laws.

The FUSD Acceptable Use Policy (“AUP”) is in place to prevent unauthorized access and other unlawful activities by Learners online, prevent unauthorized disclosure of or access to sensitive information, and to comply with the Children’s Internet Protection Act (“CIPA”). As used in this policy, “Learner” includes anyone, including employees, students, and guests, using FUSD technology, including, but not limited to, computers, networks, Internet, email, chat rooms and other forms of technology services and products. Only Learners who agree to this Acceptable Use Policy are authorized to use FUSD technology.

This policy describes acceptable uses of district technology systems (hardware, software, network, and internet) as well as unacceptable uses. These policies are established to:

- enhance teaching and learning;
- increase safety for students and staff;

- improve the efficiency of district technology systems;
- ensure alignment with FUSD Core Beliefs and Commitments;
- ensure compliance with applicable district policies, state and federal laws; and
- educate students, staff, and other who use Fresno Unified School District technology

The District will use technology protection measures to block or filter, to the extent practicable, access of visual depictions that are obscene, pornographic, and harmful to minors over the network. The District reserves the right to monitor Learners' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Learners should have no expectation of privacy regarding their use of District property, network and/or Internet access or files, including email.

Learners and other users are required to follow this policy and report any misuse of the District's technology, including network or Internet to a supervisor or other appropriate District personnel. Access is provided primarily for education and District business. Staff may use the Internet, for incidental personal use during duty-free time. By using the network, Learners have agreed to this policy. If a Learner is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a supervisor or other appropriate District personnel.

Violation of these policies may result one or more of the following: disciplinary action and/or termination for employees and temporary staff, termination of contracts for consultants or contract employees; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of access privileges, civil, and criminal prosecution. The District will attempt to tailor any disciplinary action to the specific issues related to each violation.

1. Unacceptable Uses of FUSD Technology

These are examples of inappropriate activity on the District web site, but the District reserves the right to take immediate action regarding activities 1) that create security and/or safety issues for the District, students, employees, schools, network or computer resources, or 2) that expend District resources on content the District in its sole discretion determines lacks legitimate educational content/purpose, or 3) other activities as determined by District as inappropriate.

1. Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
2. Criminal activities that can be punished under law.
3. Selling or purchasing illegal items or substances.
4. Obtaining and/or using anonymous email sites, spamming, spreading viruses.
5. Causing harm to others or damage to their property.
6. Using profane, abusive, or impolite language; 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 users' names, emails, files, or data disguising one's identity, impersonating other users, or sending anonymous email.
8. Damaging computer 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 computer to pursue "hacking," internal or external to the District, or attempting to access information protected by privacy laws.
10. Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes".
11. Using web sites, email, networks, or other technology for political uses or personal gain.
12. FUSD internet and intranet property must not be used for personal benefit.
13. Learners must not intentionally access, create, store or transmit material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others.
14. Advertising, promoting non-district sites or commercial efforts and events
15. Learners must adhere to all copyright laws.
16. Learners are not permitted to use the network for non-academic related bandwidth intensive activities such as network games or transmission of large audio/video files or serving as a host for such activities.

2. Security

1. Learners must report any weaknesses in FUSD internet and intranet security, any incidents of possible misuse or violation of this agreement to District Webmaster.
2. Every Learner provided with a Learner ID and Password must maintain their password privately and not share their password with anyone else.
3. Learners must not attempt to access any data or programs for which they do not have authorization or explicit consent.
4. Learners must not purposely engage in activity that may degrade the performance of FUSD Information Technology systems and related Information Technology property; deprive an authorized FUSD Learner access to a FUSD resource; obtain extra resources beyond those allocated; circumvent FUSD security measures.
5. Learners must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of FUSD Information Technology systems and related Information Technology property.
6. All 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 the 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 electronically transmitted the data must still be protected as confidential and secured.
7. All software programs, applications, source code, object code, documentation and data shall be guarded and protected.
8. Access to FUSD Information Technology equipment must be properly documented, authorized and controlled.

3. **Acceptable Use Policy Supporting Information**

1. FUSD Information Technology Administrators reserve the right to remove any content (organizational or personal) on the internet or intranet at any time, without cause or notice.
2. There is no guarantee of personal privacy or access to FUSD 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.
3. Schools and Departments responsible for the custody and operation of District technology shall be responsible for proper authorization and related technology utilization, the establishment of effective use, and reporting of performance to management.
4. All commercial software used on FUSD Information Technology systems are copyrighted and designated for District use. Learners must abide by all license agreements.

6. **Password Policy**

1. Passwords must not be shared with anyone and treated as confidential information.
2. Passwords must be changed at least every 180 days.
3. Passwords must have a minimum length of 8 alphanumeric characters.
4. Passwords must contain a mix of upper and lower case characters and have at least 1 numeric character.
5. Passwords must not include your employee number, name, SSN, phone number, birthday, or the name of your department or school
6. All Learners are responsible for managing their use of FUSD Information Technology systems and are accountable for their actions relating to security. Learners are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management responsible for FUSD Information Technology system security incident handling.
7. Learner account passwords shall be protected by the individual Learner from use by, or disclosure to, any other individual or organization. All security violations shall be reported to respectful security incident handling management.
8. Access to, change to, and use of Account Management Policy must be strictly secured. Access authority for each Learner must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.
9. On termination of the relationship with FUSD Information Technology Learner all security policies for FUSD apply and remain in force surviving the terminated relationship.
10. Departments and schools that have district technology must provide adequate access controls in order to monitor FUSD Information Technology systems to protect business data and associated programs from misuse. All FUSD Technology access must be properly documented, authorized and controlled, following FUSD standard processes.

4. **Incidental Use**

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

