Department of Technology
601 McAllister Street
San Francisco, CA 94102
Telephone 415-241-6476

Technology Acceptable Use and Security Policy - Employee

The Technology Acceptable Use and Security Policy ("policy") applies to all San Francisco Unified School District (SFUSD) employees and any other person or entity granted access to or use of the SFUSD's computer network and facilities, whether or not employed by the SFUSD ("Users"). To gain access to District computers, facilities, network, software applications, and the Internet, Users must review and agree to abide by the terms of this SFUSD Technology Acceptable Use and Security Policy - Employee.

1. **Educational and Business Objectives**
   District computers, networks, software applications, electronic mail, voice mail and other computer, electronic and telecommunication technologies and facilities are to be used solely for SFUSD business and educational purposes.

2. **SFUSD Property**
   All technology devices, software, and equipment configurations are owned by the San Francisco Unified School District. All files stored on SFUSD equipment and back-up devices are considered to be property of the SFUSD, and materials developed by staff in the course of carrying out their professional responsibilities on District time shall be the property of SFUSD. All equipment, software and business files must be returned immediately upon termination of employment.

   Neither the hardware nor software configuration can be changed without specific permission from the Department of Technology. Examples of changes requiring authorization include: installing new software or hardware, formatting a hard drive, adding new drivers. To request a change, submit a Service Request to the Department of Technology. Any intentional damage to the configuration of equipment may result in appropriate disciplinary actions.

   If the technology issued to a User is stolen, whether on SFUSD property, or in the User's personal possession, the User is responsible to immediately notify the police and a copy of the report must be submitted to the proper SFUSD personnel. All required equipment and software repairs should be reported to the Help Desk through the Service Request System (https://help.sfusd.edu) and repaired only by authorized SFUSD personnel.

3. **Use is a Privilege**
   Use of the District's computing and networking resources is a privilege. The SFUSD and the individual schools reserve the right to restrict or terminate network and Internet access at any time.

4. SFUSD Email

SFUSD employees must exclusively use their SFUSD-provided email account (@sfusd.edu) for email correspondence related to SFUSD business or student/educational information. Employees may not use personal email accounts or private websites for communication and interaction with students, parents and the community that relate to district/school/student matters.

5. No Expectation of Privacy

USERS OF THE SFUSD COMPUTER NETWORK SYSTEM (INCLUDING BUT NOT LIMITED TO EMAIL AND THE INTERNET) HAVE NO EXPLICIT OR IMPLICIT EXPECTATION OF PRIVACY. Any or all uses of the system and all files on the system may be intercepted, recorded, monitored, copied, deleted, audited, inspected and disclosed to authorized personnel as well as any other person or entity permitted access under the law. SFUSD shall cooperate with law enforcement agencies investigating illegal activity on the SFUSD network.

Unless otherwise stated, submission of a Help Desk call or Service Request will authorize technicians to access individual's e-mail or files as it may be necessary for technical support personnel to review the information during the course of problem resolution.

6. User Back-up

It is the User's responsibility to back up critical business data and files.

7. Internet Service Providers

While on an SFUSD site, staff must access the Internet only through the SFUSD's network. All Internet traffic must pass through the SFUSD network where access controls and related security mechanisms will be applied. Staff may not use any service to bypass the SFUSD network, security mechanism, or content filtering policies.

8. Safety

Sharing of personal information via the Internet such as name, address, and phone number, can compromise personal safety. Privacy cannot be guaranteed in a network environment.

9. Confidentiality of Information

SFUSD staff may have access to information which is confidential. SFUSD requires that staff maintain absolute confidentiality in all electronic student, employee, and application maters. Access to confidential information REGARDING DISTRICT STAFF OR STUDENTS is authorized ONLY when staff have a legitimate business need to access the information to fulfill his or her professional responsibility, and for which they have been explicitly authorized to access. UNAUTHORIZED ACCESS TO OR DISSEMINATION OF CONFIDENTIAL INFORMATION SHALL BE GROUNDS FOR DISCIPLINE UP TO AND INCLUDING TERMINATION.

10. Liability

The SFUSD makes no assurances of any kind, expressed or implied, regarding any computer or Internet services provided.

11. Appropriateness of Materials

Access to the Internet provides opportunities for staff and students to explore resources outside of the walls of their schools or offices. The SFUSD acknowledges the fact that inappropriate materials exist and will make what it judges to be reasonable and appropriate efforts to avoid such materials, including the use of filtering software. However, no software or appliance can filter out all materials that are inappropriate or unacceptable for academic purposes and it should be clearly understood by all staff, students, and students' parents/guardians that intentional access to such material, in any form, is strictly forbidden. The network is designed to achieve and support the SFUSD's business and instructional goals and any information that does not support the goals is to be avoided. If a staff or student unintentionally accesses such information while doing legitimate research, he/she should contact the person responsible for technology at his/her site for appropriate action. It is the responsibility of all users, staff and students, to ensure that SFUSD computers, the network, and the Internet are being used for educational or SFUSD business purposes.

12. Copyright

Unless it is otherwise stated, Users should assume that all materials on the Internet, including web sites and graphics, are copyrighted. Existing copyright guidelines, such as those involving photocopying, multimedia, and fair use, apply. Copyrighted material shall be posted online only in accordance with applicable copyright laws. Staff and students may not copy software on any SFUSD computer and may not bring software from outside sources for use on SFUSD equipment without the prior approval of the Department of Technology or its designee. The District shall not be responsible or liable for unauthorized use or distribution of copyrighted materials and reserves the right to seek indemnification from the User for the inappropriate use, distribution or possession of copyrighted material on the District computers or network facilities.

13. User Accounts and Passwords

- A User in whose name a network account is issued is responsible at all times for its proper use, and such User shall access the system only under the account number that has been assigned to him/her.
- Passwords must never be shared. To share a User ID or password exposes the authorized User to responsibility for actions the other party takes with the password and ID.

- Users must take reasonable steps to ensure the security/privacy of their passwords, including changing the password periodically, selecting a password that is complex and known only to the User, and never displaying the password in a public place.

14. Security

- Users may not make arrangements for, or complete the installation of, any physical or logical connection, nor make alterations to the existing SFUSD network unless approved by the Department of Technology. This includes connecting computers, servers, network electronics or other network enabled devices to the SFUSD's network.
- Users may not establish any physical or logical network connection that could allow users to gain unauthorized access to the SFUSD's systems and information. This includes the establishment of multi-computer file systems, web services, Internet, and FTP servers.
- Users may not establish any unauthorized server or file sharing mechanism, including, but not limited to, intranet servers, electronic bulletin boards, instant messaging, local area networks, modem connections to existing networks, or multi-user systems for communicating information.
- No proxies or personal firewalls are allowed.

15. Use of Wireless Devices

PDAs, Pocket PCs, cellular phones, and other wireless devices that can contain sensitive information must be secured in the same manner as desktop and laptop computers. These devices will be issued and returned according to SFUSD equipment procedures. If equipment issued to a User is lost or stolen, it is the User's responsibility to report the loss immediately. Failure to take reasonable and appropriate steps to secure sensitive information shall be grounds for discipline, including possible termination.

16. Appropriate Behavior

Staff members are responsible for appropriate behavior on the SFUSD's computers, business systems, network, and the Internet, and must adhere to all relevant federal, state, and local laws, as well as SFUSD policies and procedures.

17. Staff Working with Students

Employees working with students are responsible for supervising, at all times, students' use of SFUSD technology. Employees must enforce the Acceptable Use Policy with students under their supervision.

18. Consequences of Violations- Disciplinary Action

Any violation of the requirements and guidelines in the Acceptable Use Policy may be cause for restriction or revocation of network access privileges. Said revocation will not inhibit the District's authority to impose disciplinary action as deemed appropriate, up to and including

termination. If a staff member is accused of any of the violations listed above, he/she has all of the rights and privileges that a staff member would have if he/she were subject to any other type of disciplinary action. Users assume personal responsibility and liability, both civil and criminal, for uses of the network not authorized by this policy and the SFUSD's guidelines. The District does not sanction any use of its computer systems or the Internet that is not authorized by or conducted strictly in compliance with this policy. The SFUSD retains the right to remove from its information systems any material it views as offensive or potentially illegal.

Signature Required On Next Page

Department of Technology
601 McAllister Street
San Francisco, CA 94102
Telephone 415-241-6476

PLEASE SIGN BELOW IF YOU AGREE TO THE FOLLOWING STATEMENTS:

- I have read, understand, and agree to the SFUSD Technology Acceptable Use and Security Policy - Employee. I agree to follow all of the rules contained in this six-page document. I understand that if I violate the rules, my account can be terminated, my access to computers revoked, and I may face disciplinary measures up to and including termination.

- I understand that Internet sites are filtered and that my District email accounts and Internet use, as well as any other uses of the system or files on the system, may be monitored by the District as described above.

- I hereby release the SFUSD, its personnel and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my use of, or inability to use, the SFUSD's network and computer systems, including but not limited to claims that may arise from the unauthorized use of the system.

Employees working with students:

- I agree to enforce the Acceptable Use Policy with students under my supervision.

Employee's Name (Print)		**Employee ID No.**	
Employee's Signature		**Date Signed**	
Current or Anticipated Work Location			

Rev. 02/28/2018