St. Helena Unified School District

Acceptable Use Policy for District Technology

Overview:

Appropriate organizational use of information and information technology ("IT") resources and effective security of those resources require the participation and support of the organization's workforce ("users"). Inappropriate use exposes the organization to potential risks including cyber attacks, compromise of network systems and services, and legal issues.

The St. Helena Unified School District ("SHUSD") Acceptable Use Policy ("AUP") is to prevent unauthorized access and other unlawful activities by users 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, "user" includes anyone using the organization's information or physical infrastructure regardless of its form or format; including but not limited to computers, internet, email, chat rooms, text messages and other forms of direct electronic communications or equipment provided by the District (the "network"). Only current students and District Staff are authorized to use the network. There is a "guest" network for utilization by outside entities. It is the user's responsibility to read and understand this policy and to conduct activities in accordance with its terms.

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, intercept, record, read, copy, access, store, delete or capture in any manner including real time, users' online activities and any electronic communication or files and disclose them to others as it deems necessary (by authorized personnel without additional prior notice to individuals). Users should have no expectation of privacy during any use of the district's property or IT resources, or in any data on those resources; including but not limited to network access, Internet usage, and storage of electronic files, including email.

Definitions:

A. **District Computers:** The term "District Computer" means any computer that is owned, leased or rented by the district, purchased with funds from a grant approved or awarded to the district or school site, or borrowed by the district from another agency, company, or entity, whether or not the computer is equipped with a network interface card or communication peripheral capable of digital connection. District computers include but are not limited to:
  - Desktop Computers
  - Laptop Computers
  - Chromebooks
  - Tablets (e.g. Surface, iPads, Android Tab, etc)
  - Cellular Phones and Smartphones
  - Interactive Display Boards (e.g. Promethean, SMART, InFocus)
  - Servers

B. **Electronic Devices:** the term "District Electronic Device" means any device other than a district computer that is capable of transmitting, receiving, or storing digital media and is owned, leased, or rented by the district, purchased with funds from a grant approved by or awarded to the district or school site, or borrowed by the district from another agency, company or entity, whether or not the electronic device is portable and whether or not the electronic device is equipped with a network interface card or other communication peripheral capable of digital connection. District electronic devices include but are no limited to:
  - VoIP Phones or Telephones
  - Radios
  - Pagers
  - Cellular Hotspots
  - Digital Cameras
  - Portable Store Devices (e.g. Flash Drives, external hard drives)
  - Portable Media (e.g. CDs and DVDs)
  - Printers, Copiers, Scanners, Fax Machines, or "All-In-One" peripheral devices

C. **District Network**: The term "District Network" means the District's Wide Area Network (WAN), Local Area Network (LAN), our Verizon cellular data plan, and internet systems including wireless networks, server systems, software, email, text messages, team messaging tools, communication tools, and voicemail.

D. **District Information:** The term "District Information" or "District Data" means the personal, private, sensitive, and/or confidential information pertaining to students, staff, and the day to day operations of the district.

Acceptable Uses of the SHUSD Network:

District Staff and other users are required to follow this policy and to confirm their consent to this policy by signing and returning page 9 to their supervisor or administrator. If written consent is not received, your usage of the District Network implies consent to this policy. Network Access is provided primarily for education and district business. District Staff may use the internet for incidental personal use during duty free time provided such use is otherwise consistent with this policy. If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult their supervisor or other appropriate district personnel. Acceptable use also encompasses the following duties:

1. Protecting District Information from unauthorized use or disclosure.
2. Observing authorized levels of access:
    a. Not sharing accounts or account information.
    b. Not using other accounts to bypass restrictions.
    c. Understanding that District Staff are granted only the amount of access needed to perform their duties (Principle of Least Privilege.)
3. Immediately reporting suspected information security incidents or weaknesses to the Chief Business Official and Director of Technology and Information Systems.

Unacceptable Uses of the SHUSD Network:

These are examples of inappropriate activity on the district network, however the district reserves the right to take immediate action regarding activities that create security and/or safety issues for the district, students, District Staff, schools, network or computer resources, or that expend district resources on content the district in its sole discretion determines lacks legitimate education content/purpose, or other activities as determined by the district to be 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 the encourage other to violate the law, confidential information or copyrighted materials;
    a. Criminal activities that can be punished under law
    b. Selling or purchasing illegal items or substances
2. Unauthorized use or disclosure of personal, private, sensitive, and/or confidential information;
3. Unauthorized use of or disclosure of district information and resources;
4. Unauthorized use of or disclosure of student data;
5. You agree to not post any material or lines to any material that you know to be false and/or defamatory, discriminatory, inflammatory, inaccurate, abusive, vulgar, hateful, harassing, obscene, profane, sexually oriented, threatening, invasive of a person's privacy, or that otherwise violate any local, state, or federal law.

Unacceptable Uses of the SHUSD Network (continued):

6. Post, store, send, transmit, or disseminate any information or material that a reasonable person could deem to be objectionable, offensive, indecent, pornographic, harassing, threatening, embarrassing, distressing, vulgar, hateful, racially or ethnically offensive, or otherwise inappropriate, regardless or whether this material or its dissemination is unlawful.

7. You further agree to not transmit or otherwise make available any content that infringes any patent, trademark, copyright, or other proprietary rights of any party.

8. You also agree not to transmit or make available any content containing any "virus", "worm", "Trojan horse", "phishing", or any computer code, file or program designed to interrupt, destroy, or limit the functionality of any computer software, hardware, or telecommunications equipment.

9. Causing harm to others or damage to their property such as:
   a. 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;
   b. Using any district computer to pursue "hacking", internal or external to the district, or attempting to access information protected by privacy laws;
   c. Forwarding "chain letters" or engaging in other types of spam messaging.
   d. Forwarding information that could be considered as part of a "pyramid scheme".

10. Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:
    a. Using another's account password(s) or identifier(s);
    b. Sharing your account password(s) with any student;
    c. Interfering with other users' ability to access their account(s);
    d. Disclosing anyone's password(s) to others or allowing them to use another's account(s)

11. Using the SHUSD network or internet for commercial purposes, such as:
    a. Using the internet for personal financial gain (e.g. to buy or sell goods or services);
    b. Using the internet for personal advertising, promotion, or financial gain;
    c. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes.

12. Use of district equipment and/or district email for personal gain;

13. Connecting unapproved devices to the district's network or any IT resources. Examples of devices include but are not limited to:
    a. Printers brought from home;
    b. 3D Printers
    c. Screen casting devices (e.g. Apple TVs, Chromecasts)
    d. Streaming content devices (e.g. Amazon FireStick, Roku)
    e. AI Auto Assistants (e.g. Amazon Alexa, Google Home)

SHUSD Acceptable Use Policy

Unacceptable Uses of the SHUSD Network (continued):

14. Accessing District Information over insecure networks. (e.g. open cafe or hotel wifi)
15. Connecting to any wireless network while physically connected to the district's wired network.
16. Installing, downloading or running software that has not been approved through the district's software approval process (accessible through the SHUSD Service Desk).
17. Installing, configuring or setting up hardware that has not been approved through the district's hardware approval process (accessible through the SHUSD Service Desk).
18. Providing unauthorized third parties, including family and friends, access to the organization's IT information, resources, or facilities.

Restrictions on Off-Site Transmission, Storage, and Access of Information:

1. Users must not transmit District Information to or from personal email accounts (e.g. Gmail, Hotmail, Yahoo)
   a. Labor groups may send union specific information to and from district and personal accounts.
2. Users must not use a personal email account to conduct district business unless explicitly authorized.
3. Users must not store district information on a non-district issued device, or with a third-party file storage service that has not been approved for such storage by the organization.
   a. Google Drive, OneDrive, and the "Z" Drive are approved file storage services
   b. DropBox, SugarSync, Sync and all other alternatives are not approved for District Information storage.

User Responsibility for IT Equipment:

Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to the district and must be immediately returned upon request or at the time an employee is separated from the district. Users may be financially responsible for the value of their assigned equipment if it is not returned upon request/separation. Should IT equipment be lost, stolen or destroyed, users are required to provide a written report of the circumstance surrounding the incident. Users may be required to repay the district for the replacement value of the equipment if lost or destroyed.

Individual Accountability:

Individual accountability is required when accessing all IT resources and District Information. Everyone is responsible for protecting against unauthorized activities performed under their user ID. This includes locking the computer screen when walking away from the system, and protecting credentials (e.g. passwords, tokens, or similar technology) from unauthorized

SHUSD Acceptable Use Policy

disclosure. Credentials must be treated as confidential information, and must not be disclosed or shared

Use of Personal Computers:

The district recognizes that some staff members prefer to use their own device while at work. The district does not ban the use of personal devices, however use of a personal device comes with the following restrictions.

1. District Technology Staff will not support personal devices brought by staff members under any circumstances. This includes but is not limited to:
   a. Placing a personal device on the SHUSD_Instruction or SHUSD_Student network. Personal devices must connect to the SHUSD_Guest network.
   b. Connecting a personal device to printing resources inside the district. (e.g. your classroom printer, admin copiers, and admin color copiers)
   c. Connecting a personal device to district storage (e.g. Google Drive, OneDrive, "Z" drive.)
   d. Assisting logging in to District resources. (e.g. Aeries, Google, Outlook, etc)
   e. Assisting in the installation or troubleshooting district software. (e.g. Office 365, Adobe Creative Cloud, etc)
   f. Troubleshooting software/hardware/network issues pertaining to the personal device.
2. The district reserves the right to filter personal devices from accessing the District Network.
3. It is highly recommended that personal devices not be used to access District Information resources such as Aeries attendance or grades as the security on a personal device is unknown.
4. Users who bring a personal device and access District Information or connect to the District Network recognize that a personally owned device may subject the contents of the device and any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request.
   a. Plainly stated, if the district receives a subpoena or public records request, the district reserves the right to access your personal device to fulfill the requirements of said subpoena or public records request.
5. Users who choose to use a personal device shall abide by all applicable Board policies, administrative regulations, and this Acceptable Use Policy.

Personal Accounts on District Devices:

The district is not responsible for loss or compromise of any personal information or data if accessed using a District Device or the District Network. Personal accounts accessed online through a web browser (e.g. Chrome, Firefox, Edge) such as bank accounts, credit cards, airline mileage accounts and the like may be accessed during duty-free time so long as it does not violate the terms listed in this Acceptable Use Policy.

Personal accounts are not allowed on district cellular/smartphones. The district is not responsible for personal expenses incurred from application, music, or game purchases made using a personal account on a district phone. District Staff needing to download applications for approved work purposes (e.g. Uber for work related travel) may do so using district provided credentials.

Media-Sharing Applications:

Media-Sharing applications (e.g. Spotify, iTunes, Pandora) are not permitted for redistribution of content (e.g. playing of copyrighted music over loudspeakers, hosting "movie nights" playing copyrighted films using the District Network or District Devices). The district cannot prevent a user from accessing a personal account on a personal device and playing copyrighted media, however the district assumes no responsibility in the case of trademark infringement.

Penalties for Improper Use:

The use of district accounts, district computers, and district devices are a privilege, not a right. Misuse will result in the restriction or cancellation of an account, and collection of a district computer or device. Misuse may also lead to disciplinary and/or legal action, including dismissal from district employment, or criminal prosecution by government authorities. The district will attempt to tailor any disciplinary action to the specific issues related to each violation.

Disclaimer:

The district makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the district's network are to be borne by the user. The district also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the internet, is understood to be the author's individual point of view and not that of the district, its affiliates, or District Staff.

Compliance:

The policy shall take effect upon publication. Compliance is expected with all district policies and standards. Policies and standards may be amended at any time, and users will be notified in writing if the Acceptable Use Policy is changed. If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a district function, District Staff shall request an exception through the Chief Business Official or Director of Technology and Information Systems.

Revision History:

This policy shall be reviewed at least once every year to ensure relevancy.

DATE:	DESCRIPTION OF CHANGE(S)	REVIEWER(S)
August 19, 2021	Reviewed to incorporate NIST template language, CSBA language, and other sample policy language (K-12 school districts)	IT Team
May, 2023	Updated language. Added several new sections. Added clarification around personal/district devices. Added clarifying language.	Derrick Machado Michelle Haupt Christopher Heller

I have received, read, understand, and agree to abide by this Acceptable Use Policy, Board Policy 4040 - Employee Use of Technology, and other applicable laws/district policies and regulations governing the use of district technology. I hereby release the district of its personnel from any and all claims and damages arising from my use of district technology or from the failure of any technology protection measures employed by the district.

Signature:
_____

Name:
_____

Date:
_____