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 virus 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 and other forms of direct electronic communications or equipment provided by the District (the "network"). Only current students and employees are authorized to use the network. 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. **Definition of "District Computers":** The term "District computer" means any computer, including a laptop or tablet computer, that is owned, leased or rented by the District, purchased with funds from a grant approved or awarded to the District, or borrowed by the District from another agency, company, or entity, whether or not the computer is equipped with a modem or communication peripheral capable of digital connection.

B. **Definition of "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 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 modem or other communication peripheral capable of digital connection. District electronic devices include but are not limited to:

- Telephones
- Cellular telephones
- Radios
- Pagers
- Voice mail
- E-mail
- Text messages
- Digital cameras
- Personal digital assistants such as Palm Pilots and Blackberries
- Portable storage devices such as thumb drives (flash memory) and zip drives
- Portable media devices such as compact discs (CD's) and digital versatile discs (DVD's)
- Printers, copiers, scanners, fax machines, or "all in one" peripheral devices.

C. Definition of "District Electronic Network": The term "District electronic network" means the District's Wide Area Network (WAN), Local Area Network (LAN), and Internet systems including software, E-mail, and voice mail systems.

Acceptable Uses of the SHUSD Computer Network:

Employees and other users are required to follow this policy. Employees are required to confirm their consent to this policy. All users must follow this policy and report any misuse of the network or Internet to 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 provided such use is otherwise consistent with this policy. Examples of allowable Internet usage includes looking at the news or viewing an instructional video on YouTube. By using the network, users have agreed to this policy. If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult supervisor or other appropriate District personnel. Acceptable use also encompasses the following duties:

- Understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information;
- Protecting organizational information and resources from unauthorized use or disclosure;
- Protecting personal, private, sensitive or confidential information from unauthorized use or disclosure;
- Observing authorized levels of access and utilizing only approved IT devices or services; and
- Immediately reporting suspected information security incidents or weaknesses to the Chief Business Official.

Unacceptable Uses of the SHUSD Computer Network:

These are examples of inappropriate activity on the District network, 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;
   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 or disclosure of district information and resources.
4) You agree not to 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.
5) 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.
6) You further agree not to transmit or otherwise make available any content that infringes any patent, trademark, copyright, or other proprietary rights of any party.
7) You also agree not to transmit or make available any content containing any "virus," "worm," "Trojan horse," or any computer code, file, or program designed to interrupt, destroy, or limit the functionality of any computer software or hardware or telecommunications equipment.
8) 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; or
   c) Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes."
9) 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); or
   d) Disclosing anyone's password to others or allowing them to use another's account(s).

10) 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; or
    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.
11) Use of District equipment and or District email for personal gain.
12) Connecting unapproved devices to the district's network or any IT resources.
13) Connecting district IT resources to unauthorized networks.
14) Connecting to any wireless network while physically connected to the district's wired network.
15) Installing, downloading or running software that has not been approved through the district's software approval process (accessed through the SHUSD Service Desk).
16) Providing unauthorized third parties, including family and friends, access to the organization's IT information, resources or facilities.
17) Tampering, disengaging, or otherwise circumventing the district's IT security controls.

Restrictions on Off-Site Transmission and Storage of Information:

Users must not transmit district to or from personal email accounts (e.g. Gmail, Hotmail, Yahoo) or use a personal email account to conduct district business unless explicitly authorized. 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.

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

Use of Personal Devices:

The District will not support personal devices. If a teacher uses a personal device at school, the device will not have access to the administrative network resources, e.g., AERIES attendance and grades, printers or back-up drives. Personal devices used at work for work purposes are discoverable (able to be requested) under the California Public Records Act and other legal statutes and can be subject to subpoena. If an employee uses a personally owned device to access district technology or conduct district business, he/she shall abide by all applicable Board policies, administrative regulations, and this Acceptable Use Policy (AUP). Any such use of 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.

Personal Accounts on District Devices:

The District is not responsible for the loss or compromising of any personal information or data if accessed using a District device or the District network.

Personal accounts accessed online through a **web browser** such as bank accounts, credit cards, airline mileage accounts and the like may be accessed during duty-free time as described under the "Acceptable Use" section above.

Personal accounts accessed online through a downloaded **application** such as Uber and OpenTable are not allowed on district devices for personal use. Employees needing to download these types of applications for approved work purposes (such as using Uber or another ride sharing application for work-related travel) may do so; however only the account used for work maybe accessed on a district device.

Media-Sharing applications (Spotify, iTunes) or any other media sharing website that isn't approved for redistribution of content are not allowed on any district-issued devices (computer, iPhone, etc.) under any circumstances see item #6 under the "Unacceptable Uses" section above.

Penalties for Improper Use:

The use of a District account is a privilege, not a right, and misuse will result in the restriction or cancellation of the account. 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 employees.

Compliance:

This policy shall take effect upon publication. Compliance is expected with all district policies and standards. Policies and standards may be amended at any time. If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a district function, employees shall request an exception through the Chief Business Official.

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

---

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 and its personnel from any and all claims and damages arising from my use of district technology or form the failure of any technology protection measures employed by the district.

Signature: _____

Name: _____ Date: _____