Shasta Union High School District

COMPUTER USE GUIDELINES

Information Technology Department

Acceptable Use Policy (AUP)

05/20/16

The Shasta Union High School District's Information Technology Department (the 'District') provides technology and access to learning opportunities through telecommunications available to students and staff.

PROPER AND ETHICAL USE: Staff and students are expected to understand and to practice ethical use of computer resources.

Conditions and Rules for Use:

1. **Acceptable Use**

The purpose of the District's data and telecommunications system is to facilitate communications in support of education. The use of your account must be consistent with the educational objectives of the District.

No user may deliberately propagate a virus, worm, Trojan horse, trap-door, or any harmful program code using District resources. This District's Internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United States, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Use of District resources for illegal activity is grounds for discipline. The District will cooperate with law enforcement authorities to investigate such acts.

Users may not use the system for lobbying activities, as defined under Education Code section 7054. This provision shall not limit the use of the system by students or staff for the purposes of communicating with elected representatives or expressing views on political issues.

Use of District resources for commercial purposes is prohibited.

Plagiarism is illegal.

2. **Privilege**

The District has the authority to determine appropriate use and may deny, revoke, or suspend a user account based upon its determination of inappropriate use. Use of the District network and all of its resources is a privilege.

3. **Monitoring**

A SUHSD employee, student, or public does not have an expectation of privacy in workplace electronic communication. The District reserves the right to inspect any transmission of data or files using the District network this includes but is not limited to private cell phones, district cell phones, private laptops, district laptops, iPad, voicemail, email, PDA's, computers or any other device using the District's wired or wireless network.

The District maintains software systems to monitor and record Internet usage. Be aware that security systems are capable of recording, for every user, each World Wide Web site visit, each chat, newsgroup or e-mail message, voice mails and each file transfer into and out of the network. No user should have any expectation of privacy using District resources, including communications sent though third-party email systems. Due to staffing constraints, not all Internet usage will be monitored; however, users should be aware that upon request, supervisors may review Internet activity for any specific employee during any period of time. Attempts to bypass or evade the District filter system will be grounds for loss of Internet privileges.

4. **Network Etiquette**

Users must abide by the generally accepted rules of network etiquette. These include, but are not limited to:

- Be polite
- Use appropriate language
- **Do NOT reveal personal information, including username, password, telephone number, or address to anyone**
- Do NOT use e-mail for commercial solicitation or to conduct business unrelated to District issues
- Do NOT use e-mail to distribute hoaxes, chain letters, advertisements, rude, obscene or harassing messages

5. **Security**

A. Security on the computer system is a high priority, especially because the system involves many users. Never share your account information, including username and password. Protect your password to ensure system security and your privilege to continue using the system.

B. Please notify the Information Technology Department if you identify a security problem on the District's network. Please do not demonstrate security problems to other users.

C. Do not attempt to log on as a District system administrator. Cancellation of privileges and criminal charges may result from such activity.

D. The District may deny access to anyone identified as a security risk for having a history of problems with other computer systems.

6. **Prohibited Activities & Content**

A. Vandalism and harassment may result in cancellation of user privileges and possible criminal charges.

B. Harassment, (cyber bullying) or the persistent annoyance of another user or interference with another user's work, includes but is not limited to the sending of unwanted email or other communications. This includes during school hours, or after school at school events or movement to and from school. If a nexus exist between the cyber bullying and school, then school administration may take disciplinary action.

C. District computer resources may not be used for games research or to play games. Non-academic activities, in general, are prohibited. In addition, users are not to waste or take supplies that are provided by the District. All users agree to work in ways that will not disturb other users.

E. Giving out personal information about another person, including home address or phone number, is strictly prohibited.

F. Any use of the network for commercial or for-profit purposes is prohibited.

G. Excessive use of the network for personal business shall be cause for disciplinary action.

H. Any use of the network for product advertisement or political lobbying is prohibited.

I. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the network.

J. No use of the network shall serve to disrupt the use of the network by others.

K. Hardware and/or software shall not be destroyed, modified, or abused in anyway.

L. Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.

M. Hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviors are prohibited on the network.

N. The unauthorized installation of any software, including shareware and freeware, for use on SUHSD computers is prohibited.

O. Use of the network to access or process pornographic material, inappropriate text files (as determined by the system administrator or building administrator), or files dangerous to the integrity of the local area network is prohibited.

P. The SUHSD network may not be used for downloading entertainment software or other files not related to the mission and objectives of the SUHSD for transfer to a user’s home computer or other personal computer. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the instructional and administrative purposes of the SUHSD.

Q. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner is prohibited, except that duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC).

R. Use of the network for any unlawful purpose is prohibited.

S. Use of profanity, obscenity, racist terms, or other language that may be offensive to another user is prohibited.

T. Establishing network or Internet connections to live communications, including voice and/or video (relay chat), is prohibited unless specifically authorized by the system administrator.

U. Use of a proxy service, or proxy server is prohibited.

7. **Controversial Material**

Education, by its nature, is a controversial activity. However, it is against District policy to use district resources for access to inappropriate or offensive material. In an effort to comply with the Children's Internet Protection Act (CIPA) the District uses blocking and filtering services, which will make it difficult for students to gain access to inappropriate or offensive sites on the Internet. Users should realize, however, that it would be impossible to find and block all objectionable content on the Internet. Therefore, if a user encounters material inappropriate to an educational environment, s/he should report the URL (Internet address) to the Information Technology Department.

8. **Staff Responsibilities/Social Networking**

Employees working with students are responsible for supervising students' use of SUHSD technology and enforcing the Acceptable Use Policy. Teachers/Staff will provide developmentally and grade appropriate guidance to students as they use network resources to conduct research and other studies related to the district curriculum. Classroom use of networked resources will be in support of District educational goals. Teachers will provide alternate activities for students who do not have permission to use the Internet. Teachers/Staff should understand expectations for professional conduct extend into the online world of social networking, blogs, and other applications. Staff is strongly discouraged from "friending" current students using social networking and messaging sites such as Facebook, MySpace, and Twitter except in the context of a school project. Teachers/Staff cannot have associations with students through virtual technology if they are irregular, unprofessional, improper or imprudent in ways that negatively affect the goals of the District. Any conduct which reflects poorly upon personnel or the school district may be grounds for disciplinary action. The District has discretion in determining if conduct reflects poorly on our students, staff and the District. Conduct which reflects poorly upon the District or personnel may be grounds for disciplinary review or action.

9. **Posting of Materials on District Sites**

Shasta Union High School District computers, the District network to which they are connected, and District-funded Internet connections are provided to enhance productivity, to facilitate professional communication, and to harness the resources of the Internet in the service of the education of the students of the Shasta Union High School District.

The Shasta Union High School District web server is not a public forum. Posting permissions and posted content is maintained at the discretion of District and site administration.

Staff posting to the District web server will abide by the Shasta Union High School District Acceptable Use Policy. Staff will not:

1. use the District web site or network for personal financial gain
2. use the District web site for any fund raising without prior written administrative approval
3. use the District web site for political advertising or issue advocacy
4. use the District web site for transmitting or requesting & receiving materials inconsistent with the mission and values of the Shasta Union High School District
5. use the District web site for attempts to breach network security or transmit viruses
6. post copyrighted images, text, sound files, or software to the District web server without filing with site administration written permission from the holder of the copyright
7. post any material, text or image, allowing the identification of any individual student without prior written approval by site administration or their designee that the proposed posting meets Board criteria for parental approval of posting student information
8. post any student addresses or telephone numbers at anytime

Note: Student personal e-mail addresses (Hotmail, AOL, Yahoo mail, etc.) should not be used on District web sites. The District does not provide personal use e-mail addresses to students, but where students have contact responsibilities, appropriate e-mail addresses with joint student/staff access will be created. A fictitious example would be Suhsd.editor@suhsd.net where this account would be accessible to the student and staff advisor for use specific to the school project needing service. This facilitates tracing harassing or inappropriate e-mail directed to the school.

A. Staff with web publishing permission will post language and materials appropriate for Shasta Union High School District communications.
B. The Shasta Union High School District web server is not a forum for student expression. Staff, in accordance with administrative guidelines established at each site, will take responsibility for posting any student-generated material to the District server.
C. Staff will not link to non-district sites that are framed or formatted in such a way as to appear to be part of the District site.
D. All sites linked directly to the Shasta Union High School District Web Site will be consistent with the standards of the Shasta Union High School District and will support and be consistent with the educational mission of the District. Staff will not link to personal home pages, will not use the District site for personal web pages, and will not use the District site for links that exist only to illustrate personal interests.
E. No ‘guest books’ or response forms which allow immediate, unmediated posting by the public will be hosted on the Shasta Union High School District web site or linked to from that site.
F. Staff may not post any material to a non-Shasta Union High School District web site that uses District logos/mascots without prior written permission from school site and administration.

G. Staff may not post any material that exists as a product of their employment with Shasta Union High School District at any non-Shasta Union High School District site unless that material is also posted on a Shasta Union High School District site and meets all the criteria above.
H. Shasta Union High School District staff will use Shasta Union High School District e-mail addresses to conduct Shasta Union High School District business. Staff shall not distribute their personal, non-Shasta Union High School District e-mail addresses to parents, students, or others for contact related to their Shasta Union High School District responsibilities.
I. Staff must understand that there is no presumption of privacy for communications stored, sent, received, or accessed through Shasta Union High School District computers, networks, e-mail system, and Internet connection and that any such material may be monitored or spot-checked to ensure compliance with District policies.

10. **Computers and Software**:

Shasta Union High School District computers will be installed and maintained ONLY by authorized staff. Only the administrator at each site designated by the Director of IT, or principal in conjunction with District IT staff will be allowed to authorize installation or maintenance of either hardware or software on Shasta Union High School District computers.

A. The District has an obligation to ensure that software on its computers is being used legally according to that software's license and to ensure that any software installed do not create difficulties on the individual computer or on the District network. Staff members who wish to be authorized to install a particular piece of software on their computers or who wish to have such software installed must certify that they are using the software according to license and must register the license information with the designated administrator at each site.

    1) Multiple installations of the same license number will be assumed to violate copyright unless a multiple license provision can be demonstrated.
    2) Software not related to the mission of the Shasta Union High School District will not be installed on Shasta Union High School District equipment.
    3) 'Migrating' to an upgraded computer does not carry with it the right to 'migrate' software to that computer unless that software is wiped clean from the original computer.
    4) The SUHSD does not allow staff or students to take home District software for home use or to be installed on personal computers.

    District technical staff has the capacity to survey individual computers through the network, will remove programs not authorized for installation, and will report the incident to the appropriate site and district administration.

B. Any password protection whether at the system level or the program level must be registered with the appropriate administrator on site. The District needs the ability to access its own equipment. Care must be taken to ensure that students or other unauthorized individuals cannot change passwords; a screen saver, which can be password protected SHOULD be password protected to prevent an unanticipated lockout.

C. Screen savers, sound events, wallpaper and other system additions represent the Shasta Union High School District, as well as the individual, when found on Shasta Union High School District systems. These should avoid sexually suggestive material as well as that which might reasonably be construed as being demeaning to individuals or groups. If law, custom, or common sense would indicate that material should not be displayed in the classroom or in an office, it should not be displayed on computers in the classroom or in that office.

D. No images, sounds, or media of any sort may be added to Shasta Union High School District equipment or to materials produced through Shasta Union High School District equipment that violate copyright.

11. **Local Area, District, and Internet**

Electronic information services (Local, District-wide, and Internet) are available to students and staff in Shasta Union High School District. The Shasta Union High School District strongly believes in the educational value of such electronic services and recognizes their potential to support curriculum and to allow staff to efficiently provide educational services. The District goal in providing this service is to promote educational excellence by facilitating research, innovation, communication, and business efficiency. Staff Internet access will be granted through local area networks and District Internet connections. A set of expectations and understandings apply to all using Shasta Union High School District network services as representatives of Shasta Union High School District on the District network and on the Internet through the Shasta Union High School District Internet gateway. These include:

A. Staff must understand that all the rules of conduct described in the Shasta Union High School District Administrative Code apply during network use.

B. Staff must use assigned accounts in support of the educational goals and objectives of the District. Staff will not allow the use of assigned accounts by others. Staff must

1) not use the network, e-mail system or Internet connection for personal financial gain including commercial advertising
2) not use the network, e-mail system, or Internet connection for political or religious advocacy or on behalf of charitable organizations
3) not send any message through the network, e-mail system or Internet connection under someone else's name
4) not transmit, request, or receive materials inconsistent with the mission and values of the Shasta Union High School District
5) not attempt to breach network security or transmit viruses
6) not use the network, e-mail system, or Internet connection for sexual or other forms of harassment

C. Staff must use language appropriate for a public system in all communications.

D. Staff must respect the copyright and/or software licensing of material received through the Shasta Union High School District network, e-mail system, or Internet connection.

E. Staff must understand that there is no presumption of privacy for communications stored, sent, received, or accessed through Shasta Union High School District computers, networks, e-mail system, and Internet connection and that any such

material may be monitored or spot-checked to ensure compliance with District policies.

F. Staff must understand that as a matter of law any document pertaining to the public business on a publicly funded system is a public record.

G. Staff must understand that the public meeting provisions of the Brown Act cannot be subverted through e-mail or network conferencing.

12. **Sanctions**

Individuals who violate the terms of the *Acceptable Use Policy* will be subject to a series of sanctions through Information Technology or the Superintendent including the installation of restrictive lock-down security on their classroom workstation and restriction or revocation of District network, Internet, and/or e-mail privileges.

Additionally, sanctions may be applied by the Shasta Union High School District HR Department or SUHSD Board in accordance with established discipline policies.

13. **No Warranties**

The District makes no warranties of any kind, whether express or implied, for the services it provides. The District is not responsible for damages a user suffers. This includes, but is not limited to, loss of data through delays, no-deliveries, or service interruptions caused by the District's negligence or by the user's errors or omissions. Use of any information obtained via the District's resources is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through District resources or services. All users should consider the source and validity of information obtained online.

Disclaimer

A. The SUHSD cannot be held accountable for the information that is retrieved via the network.
B. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and will monitor messages. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.
C. The SUHSD will not be responsible for any damages you may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by our own negligence or your errors or omissions. Use of any information obtained is at your own risk.
D. The SUHSD makes no warranties (expressed or implied) with respect to:
    a. The content of any advice or information received by a user, or any costs or charges incurred as a result of seeing or accepting any information;
    b. Any costs, liability, or damages caused by the way the user chooses to use his or her access to the network.
E. The SUHSD reserves the right to change its policies and rules at any time.

14. **Proprietary Information**

There are four assets of an organization: people, processes, proprietary information, and real property. These four factors are common across all institutions, domestic or international and regardless of type, size, location, product or market. All four must be under control to prevent loss. Proprietary Information can take on many different forms, student data being the most prevalent in the district. All information data, electronic or otherwise, is the sole property of the SUHSD. No administrator, teacher, student, or employee may take SUHSD information out of the district without the express permission of the Superintendent or the Director of IT. No SUHSD information maybe sold, or otherwise communicated by any means to other entities without the express permission of the Superintendent or the Director of IT. Student transcripts are the only exemption from this procedure.

15. **SB 178 California Electronic Communications Privacy Act**
The district may obtain information from a cell phone or other electronic device through physical interaction or electronic communications with a device when the following has occurred;

1. Pursuant to a search warrant;
2. Pursuant to a wiretap order;
3. With the specific consent of the "authorized possessor" of the device;
4. With the specific consent of the owner of the device, only when the device has been reported as lost or stolen;
5. If the district, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information;
6. If the district, in good faith, believes the device to be lost, stolen or abandoned, and shall only access electronic device information to attempt to identify, verify or contact the owner or authorized possessor of the device.

The term "authorized possessor" shall mean "the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device."

All district employees who have a cell phone or electronic device owned or service paid for by the district; hear by grant the Shasta Union High School District (aka district) consent to access all district-owned electronic devices and the information created by those devices; and consent is given to the district to access all information that is sent by or to district employees.

All students who have an electronic device owned or paid for by the district; hear by grant the Shasta Union High School District (aka district) consent to access all district-owned electronic devices and the information created by those devices; and consent is given to the district to access all information that is sent by or to said device.