Scott Valley Unified School District - Information Technology
Staff Acceptable Use Policy (AUP)
2023-2024 School Year (last updated 5/12/2023)

<u>This section applies to staff and students:</u>

The Scott Valley Unified School District's Information Technology Department (the 'District') provides technology and access to learning opportunities through telecommunications available to students and staff. The purpose of the District's data and telecommunications system is to facilitate communications in support of education. This document provides the stipulations, constraints and practices that each user must agree to, for access and continued use of the District's computer and internet services. Acceptable use of your account must be consistent with the educational objectives of the District as outlined below:

1. **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. Staff and students are expected to understand and to practice ethical use of computer resources.

Misuse of district technology and district email account is subject to disciplinary account related to each violation.

2. **Monitoring**
SVUSD employees, students, nor the public have an expectation of privacy in the 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, iPads, voicemail, email, PDA's, computers or any other device using the District's wired or wireless network at the Superintendent's discretion.

The District maintains software systems to monitor and record Internet usage. Be aware that security systems are capable of recording a user's 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 through 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. (20 USC 6777,47 USC 254)

3. **Network Etiquette**
Users must abide by generally accepted rules of network etiquette, which are, but not limited to:

- Being polite and civil in all communications.
- Using appropriate language in all communications.
- Maintaining privacy by not revealing personal information, usernames, passwords, telephone numbers or addresses to anyone.
- Using email for District purposes and not commercial solicitations or to conduct personal business.
- Using email for educational purposes and not to distribute hoaxes, chain letters, advertisements.

4. **Security**

A. Maintain complete account privacy by not sharing account information, including usernames and passwords. Protect passwords and contact the Information Technology Department (IT Dept.) to request a change if you feel it has been compromised.

B. Notify the IT Dept. if you identify a security problem on the District's network. Do not demonstrate security problems to other users.

C. Logging in as a District System Administrator is prohibited and cancellation of privileges, as well as criminal charges may result from such activity.

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

5. **Prohibited Activities & Content**

Violations to any prohibited activity or content may result in cancellation of user privileges and possible criminal charges.

A. Harassment- This includes, but is not limited to: hate mail, chain letters, discriminatory remarks, and other antisocial behaviors. It also includes Cyber-bullying and/or persistent annoyance of another user or interference with another user's work, sending of unwanted email or other communications during school hours, after school hours, school events or movement to and from school. If a connection exists between the cyber bullying and school, then school administration may take disciplinary action.

B. District computer resources are for educational purposes only and may not be used for game research or to play games.

C. Supplies and products may not be removed from the District premises. Equipment must be checked out with the IT Department or Principal prior to removing from sites.

D. A user’s personal information or that of another person, including home address or phone number, may not be given out. No student information will be posted.

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

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

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

H. 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.

I. Hardware and/or software shall not be destroyed, modified, or abused in any way.

J. 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.

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

L. Accessing, processing or sharing of pornographic material, inappropriate text files (as determined by the system administrator) is prohibited.

M. The SVUSD network may not be used for downloading entertainment software or other files not related to the mission and objectives of SVUSD 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 SVUSD.

N. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner is prohibited, except where 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). (cf.6162.6 - Use of Copyrighted Materials)

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

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

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

R. No user may deliberately propagate a virus or any harmful program code using District resources.

S. 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.

T. No user shall download, install, or otherwise utilize a proxy server or Virtual Private Network (V.P.N.) while connected to the SVUSD Network.

6. Google Apps for Education (GAFE), Google Classroom, and G-Suite

The District employs the use of Google Apps for Education, Google Classroom and the G-Suite Products to help with the educational goals and objectives of Scott Valley Unified School District. All stated guidelines and policies contained in this AUP apply to all District staff and students when using any of these applications. SVUSD reserves the right to limit storage within the confines of Google Apps for student and staff accounts.

6A. Child Internet Protection Act (CIPA)

SVUSD is required to have measures in place which protect students from harmful materials. As such, SVUSD takes the following steps with student email usage: Gmail accounts are assigned to grades K-12. Grades 2-12 have email access and K-1 uses Gmail for login purposes only. Grades 9-12 can email outside the **svusd.us** domain and all accounts are to only be used for school activities. All students receive annual digital safety policy refresh courses.

6B. Children's Online Privacy Protection Act (COPPA)

SVUSD also has the duty to abide by COPPA, which limits companies from collecting personal information from children under 13. To meet this duty, Google advertising is turned off for all Google Apps for Education users, both staff and students. No personal information is collected while students are utilizing Gmail, or the Google Apps core suite which includes restricted Gmail, Google Classroom, Drive, Calendar, Docs, Sheets, Slides, and Sites.

6C. Family Education Rights and Privacy Act (FERPA)

SVUSD will act in accordance with FERPA and not use the Google Apps for Education suite to publish any confidential student records for online public view. Additionally, parents have the right at any time to investigate the contents of their student's email account, and/or their student's Google Apps for Education files. School staff is

responsible for monitoring a student's behavior online during the school day, while parents take over that responsibility at home. Students are responsible for their behavior at all times.

7. Controversial Material

Education, by nature, is a controversial activity. However, it is against District policy to use District resources for access to inappropriate or offensive materials. 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 Internet sites. 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 IT Department.

8. SVUSD District Email Policy

Each staff member and student will be assigned a district email account. Every authorized user has the responsibility to maintain the District's image and reputation. Authorized users shall use the District's designated email account for all work/business communications in which district or student issues are involved, and not for their personal use. All District email accounts are the property of Scott Valley Unified School District and there is no expectation of privacy of content.

Use of the district email account for personal use is subject to disciplinary action.

<u>The remainder of this document applies to staff only:</u>

9. **Staff Responsibilities/Social Networking**

Employees working with students are responsible for supervising student use of SVUSD technology and enforcing the *Acceptable Use Policy*. *(Appendix A)* and *Board Policy BP4040*. 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 should maintain a professional online presence and should not participate in an online relationship with current students including, but not limited to: "friending" or following students across social media platforms. This includes, but not limited to: Facebook, Twitter, Instagram, TikTok, SnapChat, Tumblr, Discord, etc. 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 negatively upon personnel or the school district may be grounds for disciplinary action. The District has discretion in determining if conduct reflects negatively on our students, staff and the District. Conduct which reflects negatively upon the District or personnel may be grounds for disciplinary review or action. Any school sponsored social media accounts should be pre-approved through site administrators and must adhere to all rules and standards of conduct.

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that blocks/filters Internet access to visual depictions that are obscene,

child pornography, or harmful to minors and that the operation of such measures is enforced (20 USC 6777, 47 USC 254)

10. **Posting of Materials on District Websites**

SVUSD 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 SVUSD.

District and school websites shall provide current and useful information regarding District programs, activities and operations. Such information shall be appropriate for both internal and external audiences. The content of websites may include, but are not limited to, District or school news, District mission and goals, agendas and minutes of Governing Board meetings, policy information, messages from the Board or administrators, information about curriculum and instruction, school, calendars, student projects, school clubs and activities, lunch menus, transportation schedules, school maps and handbooks, parent conferences, educational resources, links to other educational sites and contacts for further information.

The Superintendent or designee shall make the information contained in the School Accountability Report Card accessible on the Internet and shall ensure that such information is updated annually. (Education Code 35258)
(cf.0510 - School Accountability Report Card)

The District Webmaster and/or designees shall be responsible for the content and publication of the District website upon approval of the Superintendent or designee, who will review all content before publication or upload to the District web server or Cloud, and will regularly check links for accuracy and appropriateness. The District Webmaster will keep the web server free of outdated or unused files, and will provide technical assistance, as needed to school webmasters. The District Webmaster will take security procedures at the discretion of District and site administration. Staff posting to the District websites will abide by the SVUSD *Acceptable Use Policy*. *(Appendix A)* The staff will not:

A. Use the District websites for any fundraising without prior written administrative approval from the Superintendent.

B. Use the District websites for political advertising or issue advocacy.

C. Use the District websites for transmitting or requesting & receiving materials inconsistent with the mission and values of the SVUSD.

D. Use the District website for attempts to breach network security or transmit viruses.

E. Post copyrighted images, text, sound files, or software to the District web server or websites without filing a written permission consent form with site administration and/or holder of the copyright.

F. 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.

G. Post any student addresses or telephone numbers at any time.

H. Propagate a virus or any harmful program code using District resources. The District's Internet facilities and computing resources must not be knowingly used 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.

I. Will not post students' personal email addresses (Hotmail, AOL, Yahoo mail, etc.) on District websites.

J. 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.

K. Use District resources for commercial purposes.

L. Use Plagiarism.

M. Install unauthorized software.

N. Infringing on copyright, licenses, trademark, patent, or other intellectual property rights.

O. Use svusd.us emails for personal communication.

11. **SVUSD Websites - Additional Agreements**

A. Staff with web publishing permission will post language and materials appropriate for SVUSD communications.

B. The SVUSD websites are not a forum for student expression. Staff, in accordance with District guidelines, will take responsibility for posting any student-generated material to the District server, Cloud and websites.

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 SVUSD websites will be consistent with the standards of the 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 sites for personal web pages, and will not use the District sites 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 SVUSD website or linked to that site.

F. Staff may not post any material to a non-SVUSD website that uses District logos/mascots without prior written permission from the school site administrator.

G. Staff may not post any material that exists as a product of their employment with SVUSD at any non-SVUSD site unless that material is also posted on a District site and meets all the criteria above.

H. Scott Valley Unified School District staff will use SVUSD e-mail addresses assigned to them using the svusd.us domain to conduct Scott Valley Unified School District business. Staff shall not distribute their personal, non-Scott Valley Unified School District email addresses to parents, students, or others for contact related to their Scott Valley Unified School District responsibilities.

I. Staff must understand that there is no expectation of privacy for communications stored, sent, received, or accessed through District computers, networks, e-mail system, and Internet connection and that any material may be monitored or spot-checked to ensure compliance with District policies.

J. Employees shall not develop any classroom or work-related web sites, blogs, forums, or similar online communications representing the District or using District equipment or resources without permission from the Superintendent or designee. Such sites shall be subject to rules and guidelines established for District online publishing activities including, but not limited to: copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs, any such site shall include a disclaimer that the District is not responsible for the content of the messages. The District retains the right to delete material on any such online communications. (cf. 1113 - District and School Websites)

12. **Computers and Software**:
Scott Valley Unified School District computers will be installed and maintained ONLY by authorized staff. Only the administrator at each site designated by the IT Supervisor will be allowed to authorize installation or maintenance of either hardware or software on SVUSD 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 does 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.

B. Multiple installations of the same license number will be assumed to violate copyright unless a multiple license provision can be demonstrated.

C. Software not related to the mission of the SVUSD will not be installed on District equipment.

D. '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.

E. The SVUSD does not allow staff or students to take home District software for home use or to be installed on personal computers.

F. Any password protection whether at the system level or the program level must be registered with the site administrator. 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; including a screensaver, which can and SHOULD be password protected to prevent an unanticipated lockout.

G. Screensavers, sound events, wallpaper, and other system additions represent the SVUSD and should reflect positively. 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.

H. No images, sounds, or media of any sort may be added to SVUSD equipment or to materials produced through District equipment that violate copyrights.

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

Electronic information services (Local, District-wide, and Internet) are available to students and staff in SVUSD. The 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 these services is to promote educational excellence by facilitating research, innovation, communication, and business efficiency. Staff Internet access will be granted through local area networks, wireless services, District Internet connections, and the Siskiyou County Office of Education. A set of expectations and understandings apply to all using SVUSD network services as representatives of SVUSD network and on the Internet through the Siskiyou County Office of Education Internet gateway. These include:

A. Understanding the rules of conduct as outlined in the *Acceptable Use Policy. (Appendix A)*

B. Use assigned SVUSD domain email accounts for all school and educational email communications and to support the educational goals and objectives of the District.

C. Users shall report any security problem or misuse of services to the Superintendent or designee.

D. Avoid use of personal email account communications during school hours.

E. Avoid using the network or any component thereof for personal financial gain or commercial advertising.

F. Avoid using the network or any component thereof for political or religious advocacy on behalf of charitable organizations.

G. Avoid sending any message through the network, email system or Internet connection under someone else's name.

H. Staff must not transmit, request, or receive materials inconsistent with the mission and values of SVUSD.

I. Staff must not attempt to breach network security or transmit viruses.

J. Staff must not use the network, email system, or Internet connection for sexual or other forms of harassment.

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

L. Staff must respect the copyright and/or software licensing of material received through the SVUSD network, email system, or Internet connection.

M. Staff must understand that there is no expectation of privacy for communications stored, sent, received, or accessed through SVUSD 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.

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

O. Staff must understand that the public meeting provisions of the Brown Act cannot be subverted through email or network conferencing.

P. Employees shall not access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs.

(cf. 4030 - Nondiscrimination in Employment)
(cf. 4031 - Complaints Concerning Discrimination in Employment)
(cf. 4119.11/4219.11/4319.11 - Sexual Harassment)

14. **Sanctions**

Individuals who violate the terms of the *Acceptable Use Policy (Appendix A)* 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 SVUSD HR Department or SVUSD Board in accordance with established discipline policies. The District reserves the right to make the final decision on whether specific uses are consistent with this policy and shall be the final authority.

15. **No Warranties**

The District makes no warranties of any kind, whether expressed 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 SVUSD 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 may, at any time monitor

messages. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

C. The SVUSD 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 SVUSD 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 SVUSD reserves the right to change its policies and rules at any time.

16. **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 SVUSD. No administrator, teacher, student, or employee may take SVUSD information out of the district without the express permission of the Superintendent or the Director of IT. No SVUSD information may be 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.

I have read, understand and agree to abide by the Scott Valley Unified School District's Acceptable Use Policy:

_____

Print name on line above

_____ _____

STAFF Member's Signature *Date*