Sunol Glen Unified School District Technology and Student Acceptable Use Policy, v.2024-2025

Shay Galletti / *Superintendent & Principal*
Manuel Pallib Jr / *IT Manager*

I. Purpose

Sunol Glen Unified School District (SGUSD) provides students access to the district's internet, data and network systems. SGUSD also provides students with access to desktop computers, chromebooks, charging stations and other technology such as printers. The purpose of the network is to allow students to complete academic work, conduct research, create projects, share, and communicate while preparing them for success in high school and general education. SGUSD provides students with electronic access to a wide range of information and the ability to communicate with people throughout the world. This document contains the rules and procedures for students' acceptable use of the electronic network and its supporting infrastructure. The purpose of this AUP is also to:

1) To establish standards for the acceptable uses of the SGUSD network and SGUSD technology; 2) To prevent unauthorized and unlawful uses of the SGUSD network and SGUSD technology; 3) To comply with the Children's Internet Protection Act of 2000 (CIPA), the Children's Online

Privacy Protection Act (COPPA), the Protecting Students Digital Privacy Act, and all other applicable laws, regulations, policies and procedures.

- The SGUSD electronic network and domain (sunol.k12.ca.us), here forth known as SGUSD Technology, has been established for a limited educational purpose. The term "educational purpose" includes classroom activities, academic research, and school-related communication.
- SGUSD Technology has not been established as a public access service or a public forum. SGUSD has the right to place reasonable restrictions on material that is accessed or posted throughout the network.
- Parent/guardian permission is required for all students.
- SGUSD reserves the right to monitor all activity on its SGUSD Domain. There should be no expectation of privacy of content or communication created on or passing through the network. Students will indemnify SGUSD for any damage that is caused by students' inappropriate use of SGUSD Technology.
- Students are expected to follow the same rules, good manners and common sense guidelines that are used with other daily school activities in the use of the SGUSD Technology. Moreover, students are expected to adhere to local, state, and federal law.
- Internet users should develop practices that meet their individual learning needs and to take advantage of the network's many useful functions.
- Student files and electronic communications are not private and may be accessed by the district for ensuring proper use. All regulations will be consistent with legal standards and laws related to search, seizure, and review.
- The access and use of SGUSD Technology including, but not limited to devices, google domain, and all web access is a privilege, not a right, and inappropriate use will result in the loss of those privileges as outlined in SGUSD Technology and Student Acceptable Use Policy.

II. Authority

Source	Citation
Federal Law (USC)	- Children's Internet Protection Act (CIPA), codified at 47 U.S.C. § 254(h)(5) - Children's Online Privacy Protection Act of 1998 (COPPA), codified at 15 U.S.C. § 6501, et seq. - Neighborhood Children's Internet Protection Act, codified at 47 U.S.C. § 254(l)
Federal Regulations (CFR)	- Children's Online Privacy Protection Rule, 16 CFR Part 312
District of Columbia Law (DC Code)	- Protecting Students Digital Privacy Act of 2016, D.C. Law 21-218, codified at D.C. Code 38-831.01, et seq.
District of Columbia Municipal Regulations (DCMR)	- 5-B DCMR §§ 2500, et seq. (Student Discipline) - 6-B DCMR § 1610 (Employee Progressive Discipline)

III. Requirements

A. General

SGUSD provides and authorizes the use of the SGUSD network and SGUSD technology to students and guests. By providing and authorizing use of technology resources, SGUSD does not relinquish control over materials on the systems or contained in files on the systems. Except as described below, there is no expectation of privacy related to information stored or transmitted over the SGUSD network or in SGUSD systems—both local and virtual/cloud-based—and SGUSD reserves the right to access, review, copy, store, or delete any files stored on SGUSD technology or in SGUSD network accounts; and all communication using the SGUSD network. Electronic messages and files stored on SGUSD computers, cloud-storage or transmitted using SGUSD systems will be treated like any other school property. SGUSD staff may review files and messages to maintain system integrity and, if necessary, to ensure that users are acting responsibly. All student accounts created by SGUSD for students or created by students at SGUSD request may be monitored by SGUSD staff.

B. Network, Email and Applications

1. Network

Access to the SGUSD network, including the internet, is provided to students solely to support student education, research, and career development. Use of the SGUSD network is a privilege, not a right. Students who violate any part of this policy or related policies may be subject to cancellation of their privileges to use the SGUSD network and possible disciplinary actions. SGUSD reserves the right to prioritize network bandwidth and limit certain network activities that are negatively impacting academic and operational services. Network users are prohibited from using the SGUSD network to access content deemed inappropriate or illegal, including but not limited to content that is pornographic, obscene, illegal, or promotes violence.

SGUSD makes no guarantee that the functions or quality of the network services it provides will be free of errors or defects. SGUSD is not responsible for any claims, loss, damages, costs, or other obligations arising from use of the network or accounts. Any charges an individual incurs due to network use will be borne solely by the individual.

SGUSD is not responsible for the accuracy or quality of the information obtained through use of the system, unless the information is obtained from the SGUSD domain website. Any statement accessible on the network or the Internet is understood to be the author's individual point of view and not that of SGUSD or its employees.

2. Filters and Monitoring

As required by the Children's Internet Protection Act (CIPA), SGUSD is required to protect students from and educate them about online threats, block access to inappropriate content, and monitor Internet use by minors on school networks.[1]

SGUSD uses technology protection to block or filter internet access to visual depictions that are obscene, pornographic, or harmful to minors. Except as described in section **V.** below, SGUSD reserves the right to supervise and monitor students' online activities and to access, review, copy and store or delete any electronic information or files and disclose them to others as it deems necessary. Students should have no expectation of privacy regarding use of SGUSD property, the SGUSD computer network or the use of the Internet, files, or email while within the SGUSD network, or while accessing SGUSD cloud storage and tools, except as established by the Protecting Students Digital Privacy Act (see Section **V.** below).

SGUSD also uses a safety management system to analyze and review content found in online student file storage, inbound and outbound SGUSD email, SGUSD email attachments, links to websites and browsing activity. This system blocks potentially harmful content and images and notifies SGUSD personnel under emergency circumstances such as threat or violence to self or others.

3. Applications - Privacy & Consent

The Children's Online Privacy Protection Act (COPPA) requires operators of websites or online services directed to children under 13 years of age, and operators of other website or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age, to obtain verifiable parental consent before collecting, using, or disclosing personal information from children.[2]

When SGUSD contracts with a website or online service to collect personal information for the use and benefit of SGUSD, and for no other commercial purpose, the operator may obtain consent from SGUSD and **is not required to obtain consent directly from parents**.[3] SGUSD will provide parents notice of consent provided by SGUSD through an electronic inventory on the SGUSD website of all COPPA-compliant websites and online services SGUSD contracts with and/or requires students under 13 to access, including a link to each operator's privacy policy, and a process through which parents may exercise their right to opt out of technology. SGUSD staff are not permitted to require students under 13 to access non-COPPA compliant sites and services.

---

[1] 47 U.S.C. 254(h)(5)(B).

[2] *See* 16 CFR Part 312.5. This requirement also applies to any material change in the collections, use, or disclosure practices to which a parent has previously consented. Operators must also give parents the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties. [3] More information about complying with COPPA is available from the Federal Trade Commission here: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-q

uestions.

4. Access Control

SGUSD implements security access control measures to ensure appropriate network and technology access for all SGUSD users and to lock out unauthorized access and potential threats. SGUSD assigns student access to the SGUSD network, SGUSD domain email accounts, and SGUSD authorized applications based on grade level and school or teacher request as follows:

- *Network*: While all students are provided with personalized credentials and passwords, students in TK through Grade 4 will use school-provided generic logins, and in some cases (Gr. TK-3), QR Code login badges. Students in Grades 5-8 must use their personalized credentials and passwords to log in.
- *Email*: Students in Grades 2-8 are provided with access to SGUSD gmail. ● *Applications*: SGUSD provides access to a standard set of approved applications for all SGUSD staff and students. Staff access is provided based on job responsibility. Student access is provided by school and teacher request.

5. Passwords

SGUSD users are required to adhere to SGUSD password requirements when logging into school computers, networks, and online systems. Users are not authorized to share their password and must use extra caution to avoid email scams that request passwords or other personal information. Penalties for prohibited use may result in restrictions to network access or cancellation of accounts. Additionally, violations may result in disciplinary and/or legal action for students including suspension, expulsion, and criminal prosecution. All password change requests must be completed by IT Staff.

Student passwords are prohibited from being sent via email by any staff, student or parent. For students in Grades TK-4, passwords and QR Code badges (when applicable) are located in Aeries Parent Portal.

6. Online Safety, Digital Citizenship and Cybersecurity

SGUSD will provide students with annual lessons in digital citizenship and online safety. SGUSD may require staff to complete employee training related to cybersecurity or related topics.

C. Technology (including Computer, Laptops, Desktops and Chromebooks)

1. Device Support

SGUSD provides basic installation, synchronization, and software support for SGUSD electronic devices *only*. Devices must be connected to the SGUSD network on a regular basis to receive software updates and/or for inventory purposes. Password protection is required on all SGUSD electronic devices to prevent unauthorized use in the event of loss or theft.

2. Damage, Loss, and Theft

Students may be held financially responsible for damage, loss or theft of property due to negligence. Examples of negligence include, but are not limited to:

- ❖ damage as a result of leaving SGUSD technology in a vehicle or other location that is exposed to heat, cold, or moisture;
- ❖ damage due to spilled beverages or food; or
- ❖ theft as a result of leaving SGUSD technology unattended or in an unsecure location. Submission of a police report will remove financial liability.

Students must take reasonable measures to prevent a device from being damaged, lost or stolen. Disciplinary responses for student damage will be determined under the SGUSD discipline regulations and policies. Any infraction with a device may result in students losing the privilege of using SGUSD devices for increasing periods of time, provided that students are able to participate in and complete classwork through alternative means and are able to receive all necessary special education or English Language Learner services.

In the event SGUSD technology is lost, stolen, or damaged, users are required to immediately notify SGUSD staff. SGUSD will take all reasonable measures to recover the lost property and to ensure the security of any information contained on the device. SGUSD may choose to deploy location tracking software on devices for the purpose of locating devices identified as lost or stolen.

3. Overnight or At-Home Use by Students

SGUSD school staff may not provide students with SGUSD devices for overnight or at-home use without the express written authorization of the Superintendent. In the event that such authorization is granted, SGUSD IT Staff overseeing devices must ensure adherence to privacy requirements under the Protection of Student Digital Privacy Act. [4]

---

[4] DC Code § 38-831.03(a).

IV. Conduct & Acceptable Use

While utilizing any portion of the SGUSD network and SGUSD Google Domain, users shall not record, share, upload, post, mail, display, store, or otherwise transmit in any manner, any content, communication or information that includes, but is not limited to, the following:

A. General Unacceptable Use

- Is hateful, harassing, threatening, libelous or defamatory;
- Is offensive or discriminatory to persons based on race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, gender identity or expression, familial status, family responsibilities, matriculation, political affiliation, genetic information, disability, source of income, status as a victim of an intrafamily offense, place of residence or business, or status as a victim or family member of a victim of domestic violence, a sexual offense, or stalking;
- Posting information that, if acted upon, could cause damage or danger of disruption.
- Engaging in personal attacks, including prejudicial or discriminatory attacks including, but not limited to age, race, gender/identity, disability, and/or race.
- Harassing or bullying another person. Harassment or bullying is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending messages, that student must stop.
- Knowingly or recklessly posting false or defamatory information about a person or organization.
- Use of electronic resources or SGUSD Technology for criminal written or verbal speech or speech in the course of committing a crime, instructions on breaking into computer networks, child pornography, drug dealing, purchase of alcohol, gang activities, threats to an individual, etc.
- Using electronic resources or SGUSD Technology for written or verbal speech that is inappropriate in an educational setting or violates school rules.

- Abusing SGUSD Technology such as sending chain letters or "spamming", downloading non- educational videos or downloads.
- Accessing or sending offensive messages or pictures.
- Engaging in commercial activity. Students will not offer, provide, or purchase products or services through this network.
- Providing credit card or other financial information or conducting financial transactions over the Internet.
- Political lobbying.
- Attempting to access non-instructional SGUSD systems, student information systems, non-authorized servers, or business systems.
- Utilizing any wired or wireless network with equipment brought from home or utilizing any network unassociated with the school.
- Copying another's work with or without his/her consent. Students may not freely allow another student to copy his/her work. This is considered cheating at SGUSD. ● Copying material from the Internet and representing it as his, her, or another's own work (plagiarism). This is considered cheating at SGUSD.
- Violating copyright laws or participating in the unauthorized installation, use, storage, or distribution of copyrighted software, movies, music, or any material.
- Using or altering another user's account, password, folders, files, etc. without the other user's express permission.
- Students participating in academic assessments and projects are not allowed to use any technology or other mediums for the purpose of retrieving, exchanging, or sharing information unless approved by SGUSD. These acts are regarded as cheating and will be dealt with appropriately.

B. Handling of Equipment

- Students will respect and treat the equipment with high regard and proper care. All equipment that is the property of SGUSD has an economic and symbolic link to the school's community.
- Proper care of school equipment includes avoiding the use of food and liquid around computer equipment and other technology. Food or liquid spills can cause serious damage to computers and other equipment.
- Students will refrain from any physically harsh or violent treatment towards school equipment that could cause harm to the external cosmetics or the internal functionality of the specific equipment.
- Students may be subject to disciplinary action and/or financial responsibility, including full replacement costs, should their mishandling or misuse damage equipment beyond school/student use.

C. Vandalism and Theft

- Stickers, markers, paint or pen use, on equipment, not officially approved by SGUSD will be considered defacement and vandalism of school property.
- Students are not allowed to take computers, computer laptops, calculators, and other equipment outside of the school premises.
- Theft or vandalism of any school equipment will be treated with zero tolerance. Any thefts of this kind may lead to a school-wide or a partial lock-down of all technical equipment.
- Any malicious attempt to alter, harm or destroy data, the network, other network components connected to the network backbone, hardware or software will result in cancellation of network privileges. Disciplinary measures in compliance with the school's discipline code and policies will be enforced.

D. Technology / Hardware

- Hardware and peripherals are provided as tools for student use for educational purposes.
- Students are not permitted to relocate hardware, install peripherals or modify settings to equipment without the consent of the Technology Support Staff.

E. E-Mail

- Students will be provided with e-mail accounts to participate in academic learning opportunities and for potential electronic mail services.
- Student email accounts are restricted to send/receive within the @sunol.k12.ca.us domain only. Outside domain communication is not permitted.
- Use of electronic mail will be used for school educational purposes and may be monitored by SGUSD staff and/or administration.
- Students will not establish or access Web-based e-mail accounts on commercial services that are not authorized through the SGUSD network.
- Students will not repost or forward a message that was sent to them without the permission of the person who sent them the message.
- Students will not post private information about themselves or about another person including, but not limited to: full name, address, phone number, location, date of birth, ect.
- Students will not use equipment, network, or credentials to send or post electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

F. World Wide Web

- Students are expected to use the Internet for educational purposes.
- Access to information for students on the Internet may be screened.
- Access to the web via web proxy sites is prohibited.
- Students may be identified by the following naming convention (first name last name initial, for example: johns would be John Smith's user name). Group or individual pictures of students with student identification are permitted with parental approval.
- Material placed on student Web pages are expected to meet academic standards of proper spelling, grammar and accuracy of information.
- Material (graphics, text, sound, etc.) that is the property of someone other than the student may not be used on Web sites unless formal permission has been obtained. ● All student Web pages should have a link back to the homepage of the classroom, school or SGUSD, as appropriate.
- Students should promptly navigate away from inappropriate websites and inform their teacher of such websites.

G. BYOD: Personal Computers, Tablets, Cell Phones, and other Electronic Devices ● Students are NOT allowed to use personal devices while at school.

H. Personal Safety

- The Superintendent or designee shall provide age-appropriate instruction regarding safe and appropriate online behavior. Such instruction shall include, but not be limited to, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyber-bullying, and how to respond when subjected to cyber-bullying

- Students will not share personal contact information about themselves or others without their consent. They can share their personal information within the SGUSD domains. Personal contact information includes address, telephone, cell phone, school address, or work address.
- Students will not agree to meet with someone they have met online.
- Students will promptly disclose to a teacher or other school employee any message received that is inappropriate or makes the student feel uncomfortable.
- Students will not post personal information in social networking sites (MySpace, Facebook, Discord, Quora, Instagram, etc.) that will compromise their own or other's safety or privacy.

I. System Security

- Students are responsible for their individual email and other educational accounts and should take all reasonable precautions to prevent others from being able to use them. Under no conditions should students provide their password to another person.
- Students must immediately notify a teacher or the system administrator if they have identified a possible security problem. **Students should not attempt to identify security problems because this may be construed as an illegal attempt to gain access.**
- Students will not attempt to gain unauthorized access to any portion of the SGUSD electronic network. This includes attempting to log in through another person's account or access another person's folders, work, or files. These actions are illegal, even if only for the purposes of "browsing".
- Students will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal. ● Users will not attempt to access Websites blocked by SGUSD's filtering policy, including the use of proxy services, software, or Web sites.
- Users will not use network protocol analysis "sniffing" software, keystroke loggers, remote access technology, or any other hardware or software based method to monitor the network or another user's activity.

J. Software Applications and Files

- Software is available for students to be used as an educational resource. No student may install, upload or download software without permission from the SGUSD's Technology Support Staff.
- A student's account may be limited or terminated if a student intentionally misuses software on any school-owned equipment.
- Files stored on SGUSD Network and Google Accounts are treated in the same manner as other school storage systems. Routine maintenance and monitoring of the SGUSD electronic network may lead to discovery that a student has violated this policy or the law. Students should not expect files stored on SGUSD Technology to be private.
- Students are responsible for their own data files and should not depend on the school for storing or maintaining their data.

K. Video Conferencing, Video Chat, Audio Chat, Photography

- Video conferencing and video chat are ways that students can communicate with other students, speakers, museums, etc. from other parts of the country and the world. With videoconferencing equipment, students can see, hear, and speak with other students, speakers, museum personnel, etc. in real-time.
- Video conference and chat sessions may be saved by school personnel or by a participating school in order to share the experience.

- Students' voices, physical presence, and participation in the video conference are transmitted to participating sites during each session.

V. Privacy of Student Personal Devices & Accounts

1. General Privacy

Unless an exception described in section IV.G.2 is met, SGUSD will not take or threaten to take action against a student or prospective student, including discipline, expulsion, unenrollment, refusal to admit, or prohibiting participation in a curricular or extracurricular activity, because the student or prospective student refused to:

- Disclose a username, password, or other means of account authentication used to access the student's personal media account or personal technological device;
- Access the student's personal media account or personal technological device in the presence of school-based personnel in a manner that enables the school-based personnel to observe data on the account or device;
- Add a person to the list of users who may view the student's personal media account or access a student's personal technological device; or
- Change the privacy settings associated with the student's personal media account or personal technological device.[5]

If SGUSD or SGUSD staff inadvertently receives the username, password, or other means of account authentication for the personal media account or personal technological device of a student or prospective student through otherwise lawful mean, SGUSD and/or SGUSD staff will:

- Not use the information to access the personal media account or personal technological device of the student or prospective student;
- Not share the information with anyone; and
- Delete the information immediately or as soon as is reasonably practicable.[6]

Nothing in this section prevents SGUSD from:

- Accessing information about a student or prospective student that is publicly available; • Requesting a student or prospective student to voluntarily share specific content accessible from a personal media account or personal technological device for the purpose of ensuring compliance with applicable laws or SGUSD policies, provided the request complies with requirements of this policy;
- Prohibiting a student or prospective student from accessing or operating a personal media account or personal technological device during school hours or while on school property;
- Monitoring the usage of the SGUSD network; or
- Revoking a student's access, in whole or in part, to the SGUSD network or SGUSD technology.[7]

2. Exceptions to Privacy of Personal Media Accounts and Student Electronic Devices SGUSD staff may search a student's personal media account or personal technological device or compel a student to produce data accessible from the student's personal media account or personal technological device under the following two circumstances.

a. Policy Violation

SGUSD staff may search a student's personal media account or personal technological device or compel a student to produce data accessible from the student's personal media account or personal technological device if SGUSD staff

has a reasonable suspicion that the student has used or is using the student's personal media account or personal technological device in furtherance of a violation of SGUSD policy and a reasonable suspicion that the personal media account or personal technological device contains evidence of the suspected violation.[8]

Before conducting such a search or compelling the student to produce such data, SGUSD staff **must**:

- Document to Superintendent the reasonable suspicion giving rise to the need for the search or production; and
- Notify the student and the student's parent/guardian of the suspected violation and the data or components to be searched or that the student was compelled to produce.[9]

SGUSD may seize a student's personal technological device to prevent data deletion pending this required notification only if the pre-notification seizure period is no greater than 48 hours and the personal technological device is stored securely on SGUSD property and not accessed during the pre-notification seizure period.[10]

The search or compelled production must be limited to data accessible from the account or device or components of the device reasonably likely to yield evidence of the suspected violation and no person may be permitted to copy, share, or transfer data obtained pursuant to a search or compelled production that is unrelated to the suspected violation that prompted the search.[11]

b. Imminent Threat to Life or Safety

SGUSD staff may search a student's personal media account or personal technological device or compel a student to produce data accessible from the student's personal media account or personal technological device if doing so is necessary in response to an imminent threat to life or safety.[12]

The scope of any search or compelled production must be limited to this purpose and SGUSD must, within 72 hours of the search or compelled production, provide the student and the student's parent with a written description of the precise threat that prompted the search and the data that was accessed.[13]

---

[5] DC Code § 38-831.04(a).
[6] DC Code § 38-831.04(b).
[7] DC Code § 38-831.04(e).
[8] DC Code § 38-831.04(c)(1)(A).
[9] DC Code § 38-831.04(c)(1)(B).
[10] DC Code § 38-831.04(d).
[11] DC Code § 38-831.04(c)(1)(C)-(D).
[12] DC Code § 38-831.04(c)(2)(A).
[13] DC Code § 38-831.04(c)(2)(B)-(C).

VI. Students Rights and Due Process

A. Student Rights

- Students' right to free speech applies to communication on the Internet. SGUSD Technology is considered a limited forum, similar to the school newspaper, and therefore SGUSD may restrict a student's speech for valid educational reasons. The school will not restrict a student's speech on the basis of a disagreement with the opinions that are being expressed.
- An individual search will be conducted if there is reasonable suspicion that a student has violated this policy or the law. The investigation will be reasonable and related to the suspected violation.

B. Due Process

- SGUSD will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through SGUSD Technology.
- In the event there is an allegation that a student has violated the acceptable use regulation and policy, the student and/or parent will be provided with a written notice and/or documentation of the alleged violation.
- Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. Violations of the acceptable use regulation and policy may result in a loss of access as well as other disciplinary or legal action.
- If the violation also involves a violation of other provisions of school rules, it will be handled in the manner specified in the school rules. Additional restrictions may be placed on a student's use of his/her SGUSD Technology account.

C. Limitation of Liability

- SGUSD makes no guarantee that the functions or the services provided by or through the network will be error-free or without defect. SGUSD will not be responsible for any damage suffered, including but not limited to, loss of data or interruptions of service.
- SGUSD is not responsible for the accuracy or quality of the information obtained through or stored on the network. SGUSD will not be responsible for financial obligations arising through the unauthorized use of the SGUSD Technology.

D. Violations of this Acceptable Use Policy

- Violations of this policy may result in loss of access as well as other disciplinary, financial, or legal action. Student’s violation of this policy may be subject to disciplinary consequences, which include but are not limited to:
    - Use of SGUSD Technology **only** under direct supervision;
    - **Suspension** of network privileges;
    - **Revocation** of network privileges;
    - **Suspension** of computer privileges;
    - **Revocation** of computer privileges;
    - **Financial responsibility** for material replacement;
    - **Suspension** from school;
    - **Expulsion** from school; and/or
    - **Legal action** and prosecution by the authorities;
    - The school administrators shall determine the particular consequences for violations of this policy

VII. Requirements for Policy Implementation

All SGUSD students are required to comply with the requirements set forth in this policy when electing to access SGUSD domain networks and hardware. In order to support its implementation, SGUSD Staff is expected to make students & parents aware of required activities and timelines on an annual basis. Implementation of this policy will be reinforced through a central oversight process which includes regular data reviews, record sampling, reviews of underlying documentation, and site visits (as needed). This framework will ensure that together we build a system of continuous improvement and prevent noncompliance. For key guidance and support with questions, training, or implementation, please email: support@sunol.k12.ca.us.