San Mateo Union High School District

Student Technology Acceptable Use Policy

District Internet Use and Technology Access

Internet access is available in the San Mateo Union High School District (SMUHSD) for educational communication, research, and administrative organizational purposes. Communications via technology resources are often public, and general school rules for behavior and communications apply. It is expected that users will at all times comply with district standards and will act in a responsible and legal manner, in accordance with district standards, as well as with state and federal laws.

The Administration will take measures to assure the safety and security of students when using email, social media, and various forms of online electronic communications; prohibit unauthorized access, including hacking and phishing and other unlawful activities by minors online; prohibit unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; and restrict students' access to online materials harmful to minors.

School-Issued Devices

The SMUHSD Technology Acceptable Use Agreement must be signed by both parent/guardian and student before equipment can be issued and/or accounts are set up for the student. School-issued devices are the property of the SMUHSD and are for educational use. These devices may be collected at various times throughout the year. They will be collected at the end of each school year and/or at the termination of the student's enrollment for maintenance, cleaning, and software installation and/or upgrades. Students must return school-issued device(s) at the termination of the student's enrollment.

Taking Care of the Equipment

Students are responsible for the general care of the school-issued equipment they have been issued. Devices that are broken, damaged, or fail to work properly must be reported to the SMUHSD Helpdesk at help@smuhsd.org or the Student Helpdesk at 650-558-2480. Lost or stolen equipment should be reported immediately to the Principal's Office. Students will be entirely responsible for the cost of repairs to school-issued devices damaged intentionally or due to negligence. Continuous reports of damage will be logged and dealt with on an individual basis.

Internet Safety

In compliance with the Children's Internet Protection Act (CIPA), SMUHSD will implement filtering and/or blocking software or hardware to restrict access to internet sites containing pornography, obscene illustrations, or other materials harmful to minors less than 18 years of age. However, no filtering is foolproof, and there is still the risk that a student may be exposed to unacceptable content. If a student accidentally connects to such a site, they should contact his/her teacher/supervisor immediately. If a student sees another user accessing inappropriate sites, he or she should notify a teacher/supervisor immediately.

Cyberbullying

Students are prohibited from accessing, downloading, posting, transmitting, publishing, or displaying harmful or inappropriate matter that is obscene, disruptive, sexually explicit, or that could be construed as harassment or disparagement of any member of a group protected by State or Federal law. Cyberbullying will not be tolerated and may result in disciplinary/legal actions.

> *Harmful matter, as defined by Penal Code section 313(a), means matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest, and is matter which, taken as a whole, depicts or describes in a patently offensive way sexual conduct and which, taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.*
>
> *Cyberbullying is defined as intentional harm inflicted through electronic media and includes but is not limited to the sending or posting on the Internet, social networking sites, or other digital technologies harassing messages, direct threats, socially cruel, intimidating, terrorizing, or otherwise harmful text or images, as well as breaking into another person's account and assuming that person's identity for harmful purposes.*

Students shall not knowingly access and, without permission, read, delete, copy, or modify other users' electronic files or mail messages; interfere with other users' ability to send or receive electronic content; or forge or fraudulently use other users' electronic files or mail.

Access and Security

Some uses of the SMUSD technological resources may require an individual account with a username and password. Students identified as security risks may be denied access to these resources. Inappropriate use of these electronic resources may result in disciplinary action (including the possibility of suspension or expulsion) and/or referral to legal authorities.

1. Students are expected to safeguard all personal passwords. Sharing username and password information with others or accessing another user's files will revoke access or suspend access. Students are expected to notify an administrator immediately if they believe their student account has been compromised.
2. Students are expected to access technology only with their accounts and not to allow others to use their accounts or the accounts of others, with or without the account owner's authorization.

Privacy and Monitoring Policy

The students of the SMUHSD network must be aware that information accessed, created, sent, received, or stored on the SMUHSD network or its school sites is the property of the SMUHSD. Since technology is intended for educational purposes, students shall not have any expectation of privacy in any use of SMUHSD technology.

The SMUHSD reserves the right to monitor and record all use of SMUHSD technology, including, but not limited to, access to the Internet or social media, communications sent or received from SMUHSD technology, distance learning classes and office hours, or other uses. Such monitoring/recording may occur at any time without prior notice for any legal purposes, including record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Students should be aware that, in most instances, their use of SMUHSD technology (such as web searches and emails) cannot be erased or deleted. All passwords created for or used on any SMUHSD technology are the sole property of the SMUHSD. The creation or use of a password by a student on SMUHSD technology does not create a reasonable expectation of privacy.

Recordings

Education Code provisions that apply to learning inside the classroom also apply to distance learning. California Code, Education Code § 51512 states the following:

> *The Legislature finds that the use by any person, including a pupil, of any electronic listening or recording device in any classroom of the elementary and secondary schools without the prior consent of the teacher and the principal of the school given to promote an educational purpose disrupts and impairs the teaching process and discipline in the elementary and secondary schools, and such use is prohibited. Any person, other than a pupil, who willfully violates this section shall be guilty of a misdemeanor. Any pupil violating this section shall be subject to appropriate disciplinary action. This section shall not be construed as affecting the powers, rights, and liabilities arising from the use of electronic listening or recording devices as provided for by any other provision of law.*

Acceptable Use Agreement

Students can only access SMUHSD technological resources, including the Internet, once the student and a responsible parent/guardian sign and submit the SMUHSD Acceptable Use Agreement to the designated administrator. The combined signatures at the end of this document indicate that the student and parent/guardian have read and understand the terms and conditions of appropriate use and agree to abide by them. Unauthorized or unacceptable use of school or personal technology resources may result in suspension or revocation of personal technology privileges.

I accept personal responsibility for my use of SMUHSD's internet and technology resources and for reporting any misuse of the network to a teacher. Misuse may take many forms, but it is commonly viewed as any transmission(s) sent or received that indicate or suggest inappropriate content, unethical or illegal solicitation, racism, sexism, inappropriate language, and other issues described below.

Student Email Usage

The SMUHSD may provide students with district-issued email accounts for educational communication and collaboration. The following are guidelines and expectations for student email usage within the district.

Students may interact with external and non-district email addresses for educational purposes under the following conditions:

1. The use of the district-issued email addresses must be directly related to academic activities. This includes communication-related to coursework, projects, educational collaborations, and other school-related endeavors.
2. Students must adhere to the district's AUP and all other relevant policies and guidelines.
3. Students are advised to exercise caution and discretion when using the district-issued email and must comply with all applicable laws and regulations, including COPPA and FERPA.
4. In email communications, students are prohibited from disclosing personal information, such as addresses, phone numbers, or other sensitive data.
5. Students must not use email to engage in activities that compromise their safety or the safety of others, including sharing passwords, meeting individuals in person they've met online, or engaging in inappropriate conversations or behaviors.
6. Students are to report any suspicious or concerning emails to a school administrator, Technology Support at help@smuhsd.org, or Student Tech Support call line at 650-558-2480.

Inappropriate Uses

These include but are not limited to:

A. Conducting any activity that violates school policy, the student code of conduct, or local, state, or federal law
B. Using someone’s login account to access the computer or network
C. Any changes in hardware or software configuration
D. Sending or displaying of offensive or sexually explicit messages or pictures
E. Downloading software, music, movies, or other content in violation of licensing requirements, copyright, or other intellectual property rights
F. Engaging in any activity that is harmful to other student(s), including cyberbullying. G. Using obscene or abusive language
G. Viewing pornography or other inappropriate sites
H. Disabling, bypassing, or attempting to disable or bypass any system monitoring, filtering, or other security measures. Damaging computers, unauthorized access, or hacking of computer systems or computer networks
I. Plagiarizing another person's materials to complete an assignment
J. Accessing or attempting to access material or systems on the network that the student is not authorized to access
K. Conducting for-profit business
L. Purposefully misrepresenting yourself or others
M. Posting personal information about yourself or others

CONSEQUENCES OF VIOLATIONS INCLUDE BUT ARE NOT LIMITED TO:

1. Suspension of the District’s Network system(s) access.
2. Revocation of computer access.
3. Other disciplinary or legal action per the District policies and applicable laws.

I have read, understood, and agree to abide by the terms of the Acceptable Use Policy and Guidelines. Should I violate or misuse my access to the school district’s information and technology resources, I understand that my access privilege may be revoked and disciplinary action may be taken against me.

Student Name ____

Student ID Number (Please print) ____

Student Signature ____

Date ____

I have read and discussed the provisions of the Terms and Conditions with my student.

Parent/Guardian Signature: ____

Date: ____