SOUTH SAN FRANCISCO UNIFIED SCHOOL DISTRICT
COMPUTER SYSTEM/INTERNET/E-MAIL
ACCEPTABLE USE POLICY
SECONDARY
(STUDENT)

⑦

Instructions. *As a condition of being given access to the District's Computer System, students (and their parents or guardians) are required to read this acceptable Use Policy and agree to abide by its terms by signing the Policy. Signed Policies must be completed and returned to the school site at the beginning of every school year and/or when the user first starts using the Computer System.*

INTRODUCTION

The South San Francisco Unified School District provides technology resources to its students and staff in furtherance of its educational and business purposes. It is the District's goal to promote educational excellence in the District's schools by providing technological resources, facilitating innovation, and improving communications with the support and supervision of parents, teachers, and staff. The use of these technology resources is privilege, not a right.

In compliance with federal regulations the District maintains electronic security systems to block materials that may be inappropriate for students or classroom instruction. However, access to computers and people all over the world through the District's Computer System entails potential access to material that may not be considered to be of educational value in the context of a school setting. The district believes that the value of the information, interaction, and research capabilities available through computer technology outweighs the possibility that users may obtain material that is not consistent with the educational goals of the District.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of School District activities. All users are expected to use the District's Computer System in a responsible, ethical, safe and polite manner. Parents are strongly encouraged to be involved in their children's computer use and to guide them in ethical, safe and proper use. This document is intended to clarify the terms and conditions of access to the Computer System and expectations as to its proper use.

TERMS AND CONDITIONS

1. **COMPLIANCE WITH EXISTING LAWS, REGULATIONS AND POLICIES**

All persons using the Computer System shall comply with all applicable laws and District policies including, without limitation, laws and policies regarding freedom of speech, profanity, obscenity, privacy, copyright, and misuse of computers generally. Persons using the Computer System are required to comply with student conduct requirements generally as well as with the provisions of this Policy.

2. **DEFINITIONS**

2.1 **District Computer System.** All hardware, software, operating systems, data, data storage media, networks and related devices, and data transmission and communications equipment and services (including Internet access and e-mail).

2.2 **User Area.** A user area is comprised of that portion of the District Computer System reserved for the personal use of an individual user including, but not limited to, user data files, programs, dynamic system work areas, or any other storage of processing resources dedicated to the user.

3. **COMPUTER SYSTEM ACCESS AND USE**

3.1 **System Etiquette.** Users are expected to be courteous while using the Computer System. Users shall not send or display material that is obscene, rude, offensive, or hate-based, or that could be construed as harassing to others based on their race, national origin, gender, sexual orientation, age, disability, religion, political belief or other protected characteristic. Harassment using electronic tools will be treated as any other bullying and will result in serious consequences.

3.2 **Safe Use and Disclosure of Personal Information.** Disclosure of users' own or others' home address or telephone number information on the Computer System is prohibited. All users must abide by the Internet Safety Guidelines attached to this document when using the Computer System to access the Internet for any purpose. Users who encounter inappropriate materials by accident should immediately report to their teacher. If you fail to report, you may be held responsible for downloading prohibited materials.

3.3 **Messages.** Users should not indiscriminately address messages to broad audiences. Message addressing should be narrowly tailored to the purpose at hand. Messages should only be sent to known recipients or locations. Messages or other materials should not be sent with misleading titles.

3.4 **System Modifications.** Users may not modify or alter the Computer System in any way except under the express direction of the District's System Administrator. Users may not circumvent or attempt to circumvent the Computer System internet security system. Modification and alteration of the Computer System does not include ordinary operations involving saving and deleting user-generated files created in furtherance of District business or educational purposes.

3.5 **Privacy/Computer System Monitoring.** User information, data, and communications, including e-mails, transmitted over the Computer System or contained in any part thereof is not private or subject to privacy protections. The District reserves and shall have the right to monitor all aspects of the District Computer System, including user information, data, communications, and e-mails, for the purpose of ensuring system integrity and security, preventing system abuse, maintaining the system, and furthering legitimate educational purposes.

3.6 **Student Images, Names, and Identifying Information.** Images of students may not be displayed on the Computer System unless permission is received from the student's guardian or parent. Students may be referred to by first name only unless special circumstances warrant use of the full name and prior approval is obtained from the System Administrator and the parent or guardian.

3.7 **Downloads Scanned Materials.** Approval must be obtained from the System Administrator and the supervising teacher prior to downloading or scanning any materials into the Computer System.

3.8 **Passwords and System Security.** Users are personally responsible for keeping their passwords secure, complying with system security measures, and intentional or negligent harm they may cause to the Computer System. Sharing passwords or using the Computer System under another user's password or account number is prohibited.

3.9 **Obscene/Inappropriate Materials.** Users may not access or store obscene or other inappropriate materials on the Computer System. The District reserves the right to limit the content of information accessed or stored on the Computer System for legitimate pedagogical purposes.

4. **PERMITTED USE**

The Computer system may only be used in furtherance and support of the District's educational and business goals and purposes.

5. **PROHIBITED USE**

5.1 **Illegal Use.** Users may not process, transmit, download, or publish any material in violation of any local, State, or Federal law, including, but not limited to, the following:

a. Using the Computer System to harass or bully others (cyber-bullying).
b. Maliciously accessing, altering, deleting, damaging, or destroying any part of the Computer system.
c. Moving another user's accounts, changing another user's passwords, or using unauthorized accounts.
d. Using the Computer System to make money illegally or for illegal purposes.
e. Intentionally disrupting the Computer System.
f. Causing damage to the Computer System.
g. Circumventing or attempting to circumvent the District internet security system.
h. Using the Computer System or materials contained therein in violation of copyright, trade secret, or libel laws, or for any other illegal purpose.
i. Fraudulent conduct, including credit card fraud or electronic forgery.

5.2 **Viruses and Hacking.** Users may not upload, transmit, download, or participate in any manner in the creation, promulgation, publication or use of computer viruses or any other harmful computer programs. Users may not engage in any form of hacking. Hacking includes, but is not limited to, gaining or attempting to gain unauthorized access to computer systems and/or viewing, copying, downloading, or altering the computer programs, operating systems, data files, and any other materials contained therein. Use of viruses and hacking will result in denial of access to the Computer System and may result in further discipline as discussed in Section 9 below.

5.3 **Private Security Measures.** Users may not use any passwords, recognition codes, security access devices or methods, data encryption, or physical locking devices such as locks on any part of the Computer System without the District's prior express written consent. Users must inform the District's System Administrator in writing of all security measures they wish to use and provide keys, passwords, access codes, encryption keys, and/or other security information of materials to permit the District to obtain access to their secured areas prior to using such security devices. Permission to use such measures is revocable at any time at the District's sole discretion.

5.4 **Private Financial Gain/Business.** The Computer System may not be used for private financial gain or to operate a private business enterprise.

5.5 **Use of District Names and Symbols.** Users may not use the District's name, the name of District school sites or other facilities, or District or school logos or symbols outside of the Computer System in a manner that creates the false impression that such use is sanctioned by the District. The District reserves the right to control the unauthorized use of its name, symbols, logos, or any other proprietary materials to the extent permitted by law.

6. **INTERNET USE**

6.1 **World Wide Web Sites.** All world wide web ("web") sites that users wish to place on the Computer System are subject to prior approval by the System Administrator. The System Administrator shall review and approve inclusion of links to any other sites included in a web site on the Computer System. All Web pages created by students and student organizations on the Computer System will be subject to treatment as District-sponsored publications. The District reserves the right to exercise editorial control over such publications. Web sites the District permits to exist on the Computer System are to be deemed or operated as open forums.

6.2 **Web Access Information.** The District reserves the right to access user areas containing "cookies," web browser site access trails, or other web access information and modify or delete such items in the interests of system security, maintenance, integrity and legitimate educational purposes.

6.3 **Social Networking Sites.** Users may not access social networking sites, such as chat rooms, through the Computer System unless prior approval is obtained from the System Administrator or supervising teacher.

6.4 **Term Paper/Course Work Sites.** Accessing web sites or other sources to obtain third-party term papers or course work that is to be passed off as the user's own work is prohibited.

6.5 **Use of Credit Cards & Financial Information.** Users may not provide personal credit card or financial information of any type or conduct financial transactions over the Computer System without the prior approval of the System Administrator or supervising teacher. The District is not responsible for unauthorized costs incurred through use of the Computer System.

7. **DISCLAIMER**

The District assumes no liability, either express or implied, arising out of providing Computer system access to users. The District shall not be responsible for any damages suffered by users as a result of using the Computer System, including, but not limited to, damages suffered as the result of the user's own negligence, system delays, service interruptions, nondelivery or misdelivery of data, or the acts of other users. Use of the Computer System and information obtained therefrom is solely at the user's risk. The District makes no representation as to the content, accuracy, or veracity of any information on or obtained from the Computer system. The District disclaims any responsibility for the accuracy of information contained in or obtained from Internet service providers, or web sites, or other sources outside the Computer System.

8. **HOLD HARMLESS**

The user and the user's parent or guardian agree to release and hold harmless the District and its officers, board members, employees and agents, from and against any and all liability, loss, expense, or claim for injury or damages the user may have arising out of use of the Computer System.

9. **CONSEQUENCES OF IMPROPER USE**

9.1 **Discipline And/Or Loss Of Use Privileges.** Use of the Computer System is a privilege, not a right. Users who engage in the prohibited activities set forth in Section 5, or who use the Computer System in such a way as to violate District rules and regulations, may be subject to appropriate discipline including loss of Computer System use privileges, suspension and/or expulsion.

9.2 **Procedural Rights.** Users accused of violation of this Acceptable Use Policy shall have the same right, privileges, and disciplinary procedures to which they are entitled for infractions not related to Computer System use.

Please retain this form and the attached Internet Safety Guidelines for future reference. Indicate that you have received and read this brochure and the Internet Safety Guidelines that describes the South San Francisco Unified School District's policies of Student Image Publication/Acceptable Use Agreement by your **signature on form ①.**

If you object to any of the items listed in this document, indicate your **objection on the back of form ①.**

South San Francisco Unified School District

Internet Safety Guidelines for Students [1]

1. **There's no such thing as "private" on the Internet.** People can find anything they want if it's on-line— and keep what you post — forever.

2. **Never give personal information to anyone you meet online.** That means first or last names, phone numbers (they can be used to track down your home), passwords, birth dates or years, or credit card information.

3. **Never meet up with anyone you don't already know.** Don't tell your schedule or where you like to spend time to anyone on-line. No party announcements. People are often not who they say they are.

4. **Don't fill out any "fun" questionnaires that are forwarded to you, even if they're from your friends.** Remember, you're in a world where everything can get forwarded.

5. **Make sure you know everyone on your buddy list.** If you haven't met the people face-to-face, they may not be who they pretend to be. Also, Instant Messaging strangers is an invasion of their privacy.

6. **Don't answer emails or IMs from people you don't know.**

7. **Be careful about posting pictures of yourself.** Don't show behaviors or dress you wouldn't want your parents, teacher, boss, or potential college advisor to see.

8. **Don't send pictures of other people or rude e-mails.** Forwarding embarrassing pictures of others or rude emails is a form of bullying and will treated as seriously as face-to-face bullying. If you receive hate emails or Instant Messages or other hurtful or inappropriate materials posted on the web, tell your parents or a teacher immediately.

9. Don't **download content without your parents' permission.** Many sites have spyware that will damage your computer. Other sites have really inappropriate content. Remember, your parents can check your computer's URL history.

10. **Never share your password with anyone but your parents.**

Internet Safety Guidelines for Parents[1]

1. **Be aware and involved.** Just as we teach them how to eat properly and drive safely, we must teach them how to be safe, responsible, and respectful on the Internet.

2. **Do your homework.** Check out sites your children visit. Don't be intimidated by the Internet.

3. **Talk to your children.** Ask them questions about where they're going online and who their buddies are

4. **Teach safety.** Make sure your children know how to avoid dangers. No party postings, no personal information, no meeting strangers — ever.

5. **Set rules.** Time limits, place limits, codes of conduct. Try to keep computers with Internet access in a central room in your house if younger children are online.

6. **Report suspicious activity** to your Internet service provider or the National Center for Missing and Exploited Children (1-800-843-5678).

7. **Help children view online information with a critical eye.** Teach them to be savvy, critical consumers of Internet information.

8. **Never click on pop-ups**, and don't enter contests or answer questionnaires. At best, it opens up your computer to advertising spammers. At worst, children could share personal information with strangers.

9. **Investigate Internet safety software** that includes filters and blocks for young children. Keep Internet browsers up-to-date for virus, adware, and spyware protection.

10. **Balance your teen's need for privacy and self-expression with concerns about safety and responsibility.** Middle school and younger children should not be allowed on social networking sites. Forbidding social networking sites probably won't work for high school students, so focus your energies on appropriate postings and safety information.

11. **Cyber-Bullying**: Talk to your children about cyber-bullying. Encourage them to tell you or a teacher if they receive hate-e-mails or are harassed in any way through the Internet. Remind them that bullying using e-mail or the Internet will be treated as seriously as face-to-face bullying and carries serious consequences.

[1] Adapted from the "Internet Survival Tips for Kids and Teens" and "Internet Survival Tips for Parents and Teachers" developed by Commonsense. For more cyber-safety information go to www.commonsense.com.