District Student Acceptable Use Policy

PART A - COMPUTER USE

The Schertz-Cibolo-Universal City ISD ("SCUCISD") provides technology resources to its students for educational purposes only. The goal in providing these resources is to promote education by facilitating resource sharing, innovation, communication and responsible use with the support of parents, teachers, and staff. All users are expected to use the System in a responsible, ethical, polite manner, and in accordance with the District Policy, CQ (LOCAL), CY (LOCAL) and CQ (LEGAL).

The Internet is an association of diverse communication and information networks. It is possible that your child may run across areas of adult content and some material that might be objectionable. While the district will take reasonable steps to preclude access to such material and does not encourage such use, it is not possible for us to absolutely prevent such encounters. SCUCISD believes the value of using these resources outweighs the possibility of coming across such content.

Proper behavior is no different than in all other activities and classes. All users are expected to use the System in a responsible, ethical, polite manner and in accordance with the District Policy.
These guidelines are provided so students and parents are aware of the responsibilities students accept when they use district owned computer hardware, software, electronic mail, and social media resources.

1. Students may not use the Internet at Schertz-Cibolo-Universal City ISD (SCUCISD) without parental approval.
2. All use of SCUCISD computers and access to the Internet must be in support of education and research and be consistent with policies and goals of the SCUCISD.
3. Even with a District Internet safety plan in place, students are expected to notify a teacher or administration whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.
4. All users are expected to follow existing copyright laws. Copyright guidelines can be found in the libraries at each campus. The illegal installation of copyrighted software for use on SCUCISD computers or computing systems is prohibited.
5. Students who identify or know about a security problem are expected to convey the details to a teacher or administrator without discussing it with fellow students.
6. Any use of SCUCISD computers for commercial and/or for profit purpose is expressly prohibited.
7. The use of SCUCISD computers for product advertisement and/or endorsement or political lobbying or campaigning is prohibited.
8. Users shall not seek information on, obtain copies of, modify files, or other data, or passwords belonging to other users.
9. No use of SCUCISD computers shall serve to disrupt the use of computers by others; hardware, software and/or web pages shall not be destroyed, modified, vandalized, or abused in any way. Vandalism includes any attempt to harm or destroy data of another user.
10. Use of SCUCISD computers 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.
11. Hate mail, harassment, discriminatory remarks, pornographic references or graphics, and other antisocial behaviors are prohibited on SCUCISD computers and computing systems.
12. Users are prohibited from using SCUCISD computers and computing systems for the electronic transmission of inappropriate photographs or text material (i.e. photos showing nudity or undergarments, any inappropriate sexually explicit photo, photos showing drugs or alcohol, referring to drugs or alcohol, using vulgar language or cursing) over the Internet, such as on a personal website (i.e. Facebook or MySpace or the like), "sexting" or distribution of nude or sexually explicit photographs by cell phone and/or SCUCISD computers and computing systems, or through any other form of mass communication.
13. Use of SCUCISD computers to access or process inappropriate text and/or graphics files, or files dangerous to the integrity of the SCUCISD is prohibited.
14. Students are responsible for the proper handling and care of technology devices while in their possession returning them in good working condition.

15. Plagiarizing or using the District technology resources to engage in academic dishonesty is prohibited.
16. Users shall not attempt to bypass or disable the District's Internet filter, security systems or software.
17. THE ABOVE LIST IS NOT INTENDED TO BE ALL-INCLUSIVE.

PART B - BRING YOUR OWN DEVICE (BYOD)

SCUCISD will be allowing students in Grades 9-12 to begin bringing their own authorized technology devices (currently including Cell Phones, Microsoft Windows PC computing devices, MAC OS X 10.6+, iPads, or Android Tablets) for individual instructional use when specifically permitted by the teacher. Utilization of personal technology devices to enhance learning in the classroom will be encouraged when deemed appropriate for all students in a given classroom, and will be at the discretion of the teacher. All devices must remain powered off and put away unless directed otherwise.

1. When using the device, students must access the internet by the way of the District's filtered wireless connection. The use of private 3G/4G network access is prohibited during the instructional day.
2. Students who use personally-owned, web-enabled devices will have access to wireless Internet but will not have access to any District drives such as network folders. Student x-drives can only be accessed via District machines.
3. Students may not use any devices to record, transmit, or post photos or video of any person without their knowledge and written parental consent. Images, video and audio files recorded at school may not be transmitted or posted at any time, without the permission of a teacher or administrator. Students are not to download music, applications, or files at any time, unless directed by the teacher.
4. SCUCISD is **not** liable for any loss or damage incurred, nor can it load software or maintain/repair any student-owned device. SCUCISD Teachers will not spend time (class or before/after school) configuring devices or troubleshooting.
5. Equipment should come to school charged and ready to go. The school will not have charging stations or extra cables for charging devices at this time.
6. Students are responsible for the security of any equipment brought with them to school. All laptops and other devices should contain proper antivirus software, as well as fully-patched (updated) operating systems, and should be clearly marked with the student's full name for identification purposes. Students are required to register the device (2 max per student) through the district form.
7. Students will not loan their device(s) to another student. The user is responsible for the content contained on the device regardless of how it originated.
8. All devices brought onto an SCUCISD campus are subject to search and seizure. Improper use could result in the loss of privileges for such devices.

PART C - MONITORED USE - TRANSMISSIONS ARE NOT CONFIDENTIAL

There is no right to privacy in the use of SCUCISD computers and networks. Electronic mail transmissions and other use of SCUCISD electronic communications systems shall not be considered confidential and may be monitored at any time to ensure appropriate use for educational or administrative purposes.

PART D - EMAIL WHEN ALLOWED

1. Email should be used for educational purposes only.
2. Email transmissions, stored data, transmitted data, or any other use of the System by students shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.
3. All email and all email content are property of the District.
4. Email should only be forwarded by a student to another person that would need the information contained in the email for educational or administrative purposes that are consistent with the goals and mission of the District.
5. Never assume electronic mail is private. Messages relating to or in support of illegal activities must be reported to the authorities and the District will comply with state and federal laws, as well as court orders or subpoenas that will require disclosure.

PART E - BLOGS, PODCASTS, SOCIAL NETWORKING, AND WIKIS

Online communication is critical to our students' learning of 21st century skills. Web 2.0 tools, such as blogging and podcasting, offer authentic, real-world vehicles for student expression. As educators, our primary responsibility to students is their safety, thus expectations for classroom blogs, student-protected emails, podcasts, or other Web interactive use must follow all District-established Internet safety guidelines.

1. The use of blogs, podcasts or other Web 2.0 tools is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other Web 2.0 tools. This includes, but is not limited to, profanity and racist, sexist, or discriminatory remarks.
2. Teachers shall monitor all communication on blogs, podcasts, or other Web 2.0 tools that are used in the classroom.
3. All students using blogs, podcasts, or other web tools are expected to act safely by keeping ALL personal information out of their posts.
4. A student should NEVER post personal information on the web (including, but not limited to, last names, personal details including addresses or phone numbers, or photographs). Do not, under any circumstances, agree to meet someone you have met over the Internet in person.
5. Comments made on blogs should be monitored and - if they are inappropriate – deleted.
6. Never create a link to web sites from your blog or blog comment without reading the entire article to make sure it is appropriate for a school setting.
7. Students using Web 2.0 tools agree to not share their username or password with anyone besides their teachers and parents and to treat any Web 2.0 environments as classroom spaces.
8. Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

PART F - DISPLAY OF STUDENT WORK OR INFORMATION:

The following conditions apply to the display of student work including, but not limited to art work, class work, photographs, podcasts, projects, and writings on the District's websites or other Internet sites. Student work that has been recorded for a grade is considered an "educational record".

1. All student work or photographs to be displayed must follow the District standard and must be compliant with the dress code as described in the Student Handbook and Code of Conduct.
2. Parental consent for students under the age of 18 must be obtained prior to posting student-created work on campus and /or District Websites, social networking, and/or other Internet sites.
3. Students may not transmit pictures without obtaining prior permission from all individuals depicted, or from parents of depicted individuals who are under the age of 18.
4. Student photographs and/or student work may only be displayed according to the directory information sheet filled out by the parent/legal guardian.

PART G - CONSEQUENCES OF IMPROPER USE:

1. The student in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use. Noncompliance with the Student Acceptable Use Policy, the Student Handbook and the Code of Conduct, and Board Policy CQ may result in suspension or termination of System privileges and disciplinary actions. This may also require restitution for costs associated with the necessary repairs and/or replacement of system, hardware, or software if any damage was caused by student's noncompliance or improper use.
2. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of email and network communications are governed by the Texas Public Information Act therefore, proper authorities will be given access to their content.

I agree to abide by the Acceptable Use Policy and BYOD agreement and guidelines. I further understand that violations may result in the loss of my WiFi access and/or device privileges, and possibly other disciplinary or legal action.

Type of Device I will be bringing:

□ Microsoft Windows PC □Cell Phone □iPad □MAC OS X 10.6+
□Android □Other ________________________ □None

Signature of Student: Grade ID#

____ ______ ________________________

As a parent I understand that my child will be responsible for abiding by the above policy and guidelines. I have read and discussed this with her/him and they understand the responsibility they have while using their personal devices. In the event that he/she violates this agreement, the district may confiscate and inspect the device, and appropriately discipline my child. I understand that this user agreement must be renewed each school year.

Signature of Parent: Date:

____ ________________________________