Student Acceptable Use of Technology Guidelines

[Its] … primary goal … is to improve student academic achievement through the use of technology in elementary schools and secondary schools.

Disclaimer:
The technical information contained herein is provided to ASCIP members and nonmembers. While ASCIP makes every effort to present accurate and reliable information, use of this information is voluntary, and reliance on it should only be undertaken after an independent review of its accuracy, completeness, efficiency, and timeliness.

Version as of June 11, 2015

TABLE OF CONTENTS

STUDENT ACCEPTABLE USE OF TECHNOLOGY GUIDELINES

BACKGROUND

Districts must improve student safety related to student interconnections.

Education Code Section 234 (b) provides that "[i]t is the policy of the State of California to ensure that … local educational agencies … work to … improve pupil safety at … the connections between pupils."

GOAL

The purpose of these guidelines is to assist Districts and their students in the appropriate use of a variety of electronic communications and information technologies (hereafter, "technology") that incorporate computer/network/Internet access. Districts strongly believe that the positive benefits of these digital resources and the information and interaction available through computers/networks/the Internet outweigh their disadvantages. When properly used, these technologies promote educational excellence in Districts by facilitating resource sharing, innovation, and communication. Illegal, unethical, or inappropriate use of these technologies can have negative consequences. In order to minimize Districts' liability and to minimize potential harm to Districts, their students, and their employees, ASCIP's Student Acceptable Use of Electronic Devices Guidelines provide a tool to minimize the likelihood of such harm by educating Districts' students, staff, teachers, and other stakeholders and setting standards which serve to protect Districts.

DEFINITIONS

For purposes of these guidelines, "**personal electronic device**" means any device in the possession of a student which electronically communicates, sends, receives, stores, reproduces, or displays voice, text, and/or digital communications or data. This includes, but is not limited to, cellular phones, pagers, smart phones, music and media players, gaming devices, tablets, laptop computers, cameras, video cameras, smart watches, headphones, ear buds, personal medical devices (PMDs), and personal digital assistants. In these guidelines, furthermore, the word, "**technology**," may be used as a synonym for personal electronic device,

For purposes of these guidelines, "**instructional day**" means the period of time between the first scheduled bell and the last scheduled bell of the school day and any other time in which instruction occurs.

GENERAL PROVISIONS

ASCIP recognizes that Districts provide essential computer related technology resources to their students for educational purposes. The goal of providing these resources is to promote educational excellence. The use of District technology resources should be granted to students for the enhancement of education-related functions. Individuals who use the District network should consent to be monitored.

ASCIP recommends that Districts use multiple layers ofl procedures to ensure students are protected while using the Internet including, but not limited to, web site filtering. Districts should comply with the federal Children's Internet Protection Act (CIPA) to address concerns about access to **inappropriate content**[1] over the Internet on school and library computers.

It is important to understand that no filtering system is perfect. Due to the nature of the Internet and evolving technology, even with supervision, Districts cannot guarantee that students will not access inappropriate content. It is be the student's responsibility to report any inappropriate site or posting to a school administrator or teacher.

The guidelines delineated below outline appropriate use and prohibited activities when using all technology resources and electronic devices.[2] Every student should follow all

[1] "*Inappropriate content*" should be based on **Local Determination of Content.** Determinations about what information is inappropriate for minors should be made by District Trustees after consideration of and in coordination with local input. In the administration of subsection 47 U.S.C. § 254(h)(1)(B), no other agency or instrumentality of the government may (a) establish criteria for making such determination; (b) review agency determination made by the certifying District Trustees; or (c) consider the criteria employed by the District Trustees.

[2] For Districts choosing to ban private electronic device use from their campuses, the following wording should be considered*: The District does not encourage student possession or use of electronic devices on school campuses, nor does it assume liability of such devices that are damaged, lost, or stolen. The use of electronic devices, such as beepers, pagers, and cellular telephones, including cellular camera phones, by students is prohibited on school premises, at all school sponsored activities, on buses, and at any time while students are under the supervision and control of district employees. An exception to this policy is the use of electronic devices essential for the student's health as determined by a licensed physician or surgeon, and the use of such device under those circumstances is limited to those purposes related to the student's health as determined by such licensed physician or surgeon. For a student to be authorized to carry an electronic signaling device for this purpose, the parent/guardian must submit a Student Use of Electronic Device for Medical Purposes form signed by a licensed physician or surgeon, indicating the type of device that is essential to the student's health and stating when and under what circumstances the student should use the device while on school premises, at school sponsored activities, or at any time while under the supervision or control of district employees. The device must remain in silent mode during instructional time and during school activities. Use of the device during instructional time is prohibited except as specifically directed in writing by the physician. The District reserves the right to confirm medical need with the physician. Such devices must not disrupt the educational program or school activity and may not be used for any activities not related to the student's health. The use of cameras, camera phones, and other devices that can take*

of the rules and conditions listed.

SAMPLE DISTRICT POLICY ON STUDENT ACCEPTABLE USE OF TECHNOLOGY

Note that optional language is in **[bracketed bold red]** type.

Rights and Responsibilities[3]

Students who possess personal electronic devices shall be solely responsible for their use and care.[4]

Possession of personal electronic devices by students **[in grades [2/3/4/5/6] through 12]** on **[all/middle and high/high]** school campuses, including on athletic fields, on school buses, at school-sponsored activities, and while the student is under the supervision and control of District employees shall be permitted. All permitted students may use these devices on campus before school begins and after school ends. In addition, **[high school/middle and high school]** students may use such devices during their lunch **[or free]** period**[s]** as determined by the school administration.

These devices shall be kept **[out of sight/in a pocket, purse, or backpack]** and powered off or silenced during the school day and during any school-sponsored activity meeting or practice held on [District] property. The requirement that personal electronic devices be turned off may not apply in the following circumstances when the student obtains prior

photographs or video recordings are prohibited on school premises except with the written permission of a teacher or administrator for use in connection with an instructional or school-sponsored activity. Items used in violation of this policy will be confiscated and, if reasonable suspicion exists, may be subject to search by an administrator, including, but not limited to, viewing pictures stored on the device or attached to text messages or email sent to or from the device. Taking photographs on school grounds or during school activities is prohibited except with the written permission of a teacher or administrator. Photographs taken without the knowledge and consent of each person being photographed are prohibited. Photography and video or audio recording in classrooms is prohibited without the prior consent of the teacher and the principal of the school, which may be given to promote an educational purpose. (Education Code § 51512).

[3] Generally, student use of personal electronic devices (*with the exception of cyber bullying or similar threats*) is a matter of applicable laws and parental/guardian rules and discipline (i.e., *not under District control*) during **non-school hours** when using an **off-campus Internet connection** on a **non-school computer or other electronic device** involving a **non-school e-mail address**.

[4] The **Privacy Rights for California Minors in the Digital World Act** (effective January 1, 2015) and **COPPA** (the federal Child Online Privacy Protection Act of 2013) were passed to help protect the privacy of minors who are digital and/or mobile consumers by prohibiting certain forms of advertising and of collection of consumer information, respectively, that serve to target individual minors. As of these Guidelines' publication, COPPA has been ineffective in stopping mobile app firms from collecting user information. Parents and Districts should be aware of potential student privacy concerns as a result of smart phone use (as well as other Internet-connected devices on private networks). Some awareness of the behaviors of mobile apps with respect to information use can be obtained though use of PrivacyGrade (see http://privacygrade.org/).

approval from the principal or his/her designee:

- The student has a special medical circumstance for self or family member.
- The student is using the device for an educational or instructional purpose with the teacher's permission and supervision.

Personal electronic devices shall be permitted on school buses, as authorized by the driver, unless use of the personal electronic device causes a disruption on the school bus.

Student use of personal electronic devices shall be prohibited in areas including, but not limited to, locker rooms, classrooms, bathrooms, and swimming pool areas. The requirement that personal electronic devices be prohibited in these places may not apply in the following circumstances when the student obtains prior approval from the principal or his/her designee:

- The student has a special medical circumstance for self or family member.
- The student is using the device for an educational or instructional purpose with the teacher's permission and supervision.

Students shall not use personal electronic devices on school property or at a school-sponsored activity to access and/or view internet websites that are otherwise blocked to students at school. **[Blocked sites include, but are not limited to:**

- **Creepy (See http://ilektrojohn.github.io/creepy/)**
- **Ask.fm (See http://ask.fm/)**
- **Vine (See https://vine.co/**
- **Snapchat (See https://www.snapchat.com/)**
- **Kik (See http://kik.com/)**
- **Pheed (See https://www.pheed.com/)**
- **Qooh.me (See http://qooh.me/)**
- **Oovoo (See http://www.oovoo.com/home.aspx)**
- **Facebook (See https://www.facebook.com/)**
- **Twitter (See https://twitter.com/?lang=en)**
- **Yik Yak (See http://www.yikyakapp.com/)**
- **Tinder (See http://www.gotinder.com/)**

- **Paktor (See http://www.gopaktor.com/)**
- **Voxer (See http://www.voxer.com/)**
- **Whisper (See http://whisper.sh/)**
- **Tumblr (See https://www.tumblr.com/apps)**
- **Instagram (See http://instagram.com/)**
- **Shots (See https://shots.com/)**
- **Cydia (See https://cydia.saurik.com/)**
- **Spring (See http://spring.me/)**
- **Youtube (See https://www.youtube.com/)]**

- The student in whose name an on-line services account is issued shall be responsible for its proper use at all times.
- Students shall keep personal account numbers, home addresses, and telephone numbers private.
- Students shall use the system only under their own account number. Passwords are private and not to be shared with others.
- The District's system shall be used only for purposes related to education.
- The District reserves the right to monitor any on-line communications for improper use. Electronic communications and downloaded material, including files deleted from a user's account, may be monitored or read by District officials or their appointees.
- Inappropriate use may result in a cancellation of network privileges.
- Only appropriate language shall be used in email, online postings, and other digital communications with others.
- Technology resources shall be used responsibly.
    - The network shall not be used for illegal or commercial activities.
    - Users shall not search, retrieve, save, circulate or display hate-based, offensive, sexually explicit, or images or information about weapons.
- Students shall be prohibited from accessing, posting, submitting, publishing, or displaying harmful matter or material that is threatening, cyber-stalking, obscene, disruptive, or that could be construed as harassment or disparagement of others

based on their race, national origin, sex, sexual orientation, sexual identity, age, disability, religion, or political beliefs.

- Students shall not use the system to encourage the use of drugs, alcohol, weapons, or tobacco, nor shall they promote unethical practices or any activity prohibited by law or District policy.
- Vandalism will result in the cancellation of user privileges. Vandalism includes the intentional uploading, downloading, or creating computer viruses and/or any malicious attempt to harm or destroy District equipment or materials or the data of any other user.
- Students shall not assume another person's identity.
- Students shall report any security problems or misuse of the services to the teacher, principal or other District employee.
- Both student and parent or legal guardian shall sign Acceptable Use Agreements before a student can use the District network.
- Students who fail to abide by the District's rules shall be subject to disciplinary action, revocation of the user account, and legal action, as appropriate.
- Students shall not make any attempt to circumvent network security.
- Student use of personal electronic devices that disrupt the instructional day may result in disciplinary action and/or confiscation of the personal electronic device. When a personal electronic device is confiscated, it shall only be released and/or returned to **[the student/the student's parent/legal guardian]**. It is the **[student's/the student's parent/legal guardian's]** responsibility to retrieve the device according to school procedures.

Acceptable Use of Networks, Including Social Media

Student use of social media or social networking that disrupts the instructional day may result in disciplinary action. Proper behavior, as it relates to the use of computers, is no different from proper behavior in all other aspects of District activities. All users shall use computers and computer networks in a responsible, ethical, and polite manner. Violation of these Guidelines shall be grounds for school disciplinary action.

Acceptable Use of Email

Email services and systems may be provided by District. The data stored in these systems shall be considered, at all times, the property of District. As such, all messages created, sent, received, or stored in the systems shall be considered the property of

District, except for any data covered by copyright or other legal property protection. Students shall not read other users' email or files; they shall not attempt to delete, copy, modify, or forge other users' mail.

Acceptable Use of the Internet

The Internet and other on-line resources provided by District is provided on an "as is" and "as available" basis and shall be used to support the instructional program and further student learning. The goal of providing these resources is to promote educational excellence.

The Internet is a network of many types of communication and information networks. While this creates new opportunities for learning, research, communication and collaboration, it also creates new responsibilities for District students.

Acceptable Use of the Cloud

The use of cloud-based storage services such as Google Drive and Dropbox is increasing. It is important to note that such services are inherently less secure than traditional storage on District servers. Passwords and logins can be saved to the cloud without your explicit consent. Therefore, it is required that the following rules are observed when using cloud storage:

1. Do not use cloud storage services to store sensitive, confidential, or personal information.[5]
2. Cloud storage services must be in compliance with District policies and procedures related to storage of District Records.

[5] Please remember that most student information is subject to the Family Educational Rights and Privacy Act (FERPA) and should not be saved in the Cloud by District personnel.

Acceptable Use of the Internet of Things (IoT)[6]

The District's provision of internet connections and wireless network services to its students and others is offered only on "as is" and "as available" bases. This has been stated in the District's annual written disclosure to all students, and this information is posted at all times on school sites. District cannot guarantee the security or availability of its systems with respect to personal medical devices (PMDs). PMD users should not rely upon the security and availability of the District's internet connections and wireless network services, and PMD users with continuous, critical needs should arrange for redundant, secure communications systems.

[Internet Safety Education

[District] Internet safety includes Internet safety education. Specifically, Internet safety education shall include lessons on cyber-bullying awareness and response as well as teaching appropriate online behaviors for students. Students shall be instructed in appropriate use of [District] technology resources.]

Student Internet Safety

Students shall not disclose their full name or any other personal contact information for any purpose on the Internet. Personal contact information includes address, telephone, or school address. Students shall not share or post privacy-revealing personal information about themselves or other people. Students shall tell their teacher or other school employee about any message they receive that is inappropriate or makes them feel uncomfortable. Students should not delete the message until instructed to do so by a staff member. Students should not provide their passwords to anyone under any condition. Students must immediately tell their teacher if their password is lost or stolen, or if they think someone has gained unauthorized access to their accounts.

Copyright Violations

[6] IoT are physical devices (hardware) that are connected to the Internet through an Internet Protocol (IP) interface. These connected devices can send and receive data over standard communications networks. Through sensors that send or receive information from data streams and/or databases and process the incoming and outgoing data, IoT can respond to or anticipate a user's needs and preferences. Potentially, IoT can provide us with tools for safer, healthier, more productive, more efficient, and/or more adaptable lives. For example, PMDs are IoT that assist in monitoring and improving our health and wellness. PMDs are medical devices that transfer medical information through the Internet. They comprise one of the most rapidly growing areas in the field of telemedicine. PMDs help monitor diabetes, chronic obstructive pulmonary disease (COPD), congestive heart failure, and hypertension in real time, thus enabling faster response to negative indications. Examples of current PMDs include thermometers, pulse oximeters, blood pressure cuffs, pedometers, weight scales, fitness equipment, medication schedule trackers, and glucose meters.

Copying, selling or distributing copyrighted material without the express written permission of the author or publisher (users should assume that all materials available on the Internet are protected by copyright) and engaging in plagiarism (using other's words or ideas as your own) shall be prohibited, and, in most cases, is illegal.

Privacy

Network and Internet access shall be provided as a tool for education. District shall reserve the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of District and no student shall have any expectation of privacy regarding such materials.

Corrective Action

Corrective action shall be determined by the number of previous acts, the nature of the act, and the context in which the alleged act occurred. Consequences may range from positive behavioral interventions to suspension and expulsion for repeated and/or severe violations.

Unauthorized Use

Unauthorized use of personal electronic devices includes, but is not limited to, the following:

1. Possessing, viewing, sending or sharing video or audio information having sexual, violent, or threatening content on school grounds, school events or school busses.
2. Transmitting school materials for unethical purposes such as cheating.
3. Any activity which may be in violation with the District Bullying Prevention Guidelines and procedures.

These uses shall be prohibited and may result in disciplinary action and/or confiscation of the personal electronic device.

District Rights and Responsibilities

District shall not be responsible for the theft, loss or damage to personal electronic devices brought to school by a student while the device is under the student's care and control. **[The school where a personal electronic device is confiscated shall be responsible for the theft, loss, or damage of personal electronic devices if the District employee demonstrated reckless disregard for internal procedures developed by the school. The school shall be responsible for the theft, loss, or damage of personal electronic**

devices confiscated by District staff if the school has not developed internal procedures.]

[The school shall develop internal procedures for staff concerning confiscation of personal electronic devices. These procedures shall include, but are not limited to, expectations that the staff will immediately secure the device, turn the device into the school designated location, develop a process for students/parents/legal guardians to retrieve devices, and record when the device was confiscated and why.]

District staff may confiscate personal electronic devices when such devices are being used in violation of **[these Guidelines and/or internal]** school procedure. Upon confiscation, District staff shall follow all District and school procedural directives and processes.

District staff may search confiscated personal electronic devices and examine the content of students' personal electronic devices when there is **reasonable suspicion**[7] of unauthorized or illegal use of the devices and may turn the devices over to the proper authorities for further investigation when warranted. When determining if a search is appropriate, District staff shall ensure the following conditions are met before conducting the search:

- The search is reasonable at its inception. That is, when the context is such that it is clear that the *specific student* or the *specific group of students* are clearly misusing the device(s) and that the search of content would turn up evidence of the violation.
- The scope of the search of the content is reasonably related to the objective of the search and appropriate in light of the age and sex of the student and the nature of the suspected violation.

[7] The Supreme Court (New Jersey v. T. L. O.) has said that school officials may search a student or a student's property if they have a **reasonable suspicion** that the search might uncover evidence that the student violated a school rule. For example, reasonable suspicion might be based on a school official overhearing, seeing, or smelling something first-hand, or on a tip from a reliable source. School officials also must be reasonable in the way they search, based on the student's age and for what they are searching. However, if a student voluntarily consents to a search, the school does not need even reasonable suspicion to conduct the search. For students who are minors, parental/guardian consent as well as student consent must be obtained before a search *unless* reasonable suspicion is present. Note also that reasonable suspicion must be individualized. If, for example, the teacher has a ***reasonable suspicion* that *someone*** has been selling drugs or alcohol via text messages, it does **not** mean that everyone's cell phone can be searched. School officials must have a reasonable suspicion that a search of a particular student will uncover evidence of a violation of a school rule.

Legal References:

EDUCATION CODE
§ 51006 Computer education and resources
§ 51007 Programs to strengthen technological skills
§ 51870-51874 Education technology
§ 60044 Prohibited instructional materials

PENAL CODE
§ 313 Harmful matters
§ 502 Computer crimes, remedies
§ 632 Eavesdropping on a recording confidential communications
§ 653.2 Electronic communication devices, threats to safety

UNITED STATES CODE, TITLE 15
6501-6506 Children's Online Privacy Protection Act (COPPA)

UNITED STATES CODE, TITLE 17
1701 Children's Internet Protection Act (CIPA)

UNITED STATES CODE, TITLE 20
6751-6777 Enhancing education through technology act, Title II, Part D

UNITED STATES CODE, TITLE 47
254 Universal service discounts (E-rate)

CODE OF FEDERAL REGULATIONS, TITLE 47
54.520 Internet safety and technology protection measures, E-rate discounts

Agreement for Acceptable Use of Networks, Including the Internet
Parent or Guardian

As the parent or guardian of _____, I have read the **[District]** Student Acceptable Use of Technology and I have discussed it with my child. I understand that computer access is provided for educational purposes in keeping with the academic goals of **[District],** and that student use for any other purpose is inappropriate. I recognize it is impossible for **[District]** to restrict access to all inappropriate materials, and I shall not hold the school responsible for materials acquired on the school network. I hereby give permission for my child to use technology resources at **[District]**. I further understand that use of District networks, including, but not limited to, the Internet are on an "as is" and "as available" basis.

Parent or Guardian's Name (please print): _____

Parent or Guardian's Signature: _____

Date: _____

Agreement for Acceptable Use of Networks, Including the Internet
Student

I understand and will obey the rules of the **[District]** Student Acceptable Use of Technology. I will use **[District]** technology resources productively and responsibly for school-related purposes. I will not use any technology resource in such a way that would be disruptive or cause harm to other users. I understand that consequences of my actions could include possible loss of computer privileges and/or school disciplinary action and/or prosecution under state and federal law. I understand that **[District]** administrators will deem what conduct is inappropriate use if such conduct is not specified in this agreement. I further understand that use of District networks, including, but not limited to, the Internet are on an "as is" and "as available" basis.

Student Signature: _____
Student Name: _____
Date:_____

Permission for Student Use of Electronic Devices on School Property Related to Special Medical (or Other) Circumstances Form

1. I understand that _____ School District maintains a policy such that students with serious medical conditions as determined by a licensed physician[8] will be allowed to possess and use a cellular telephone or other personal electronic device (PED) that is determined by a licensed physician to be essential for the health of the student. Use of the device during the school day shall be restricted to the immediate health concerns of the student. As part of this policy, the District requires signatures from the parent/legal guardian, the physician's signature, and the principal's signature before the student is allowed to carry an electronic communication device on school property. I further understand that use of PED or other devices on District networks, including, but not limited to, the Internet is on an "as is" and "as available" basis.

2. Principals are authorized to give permission for a student to possess and use a cellular telephone or other PED under highly unusual circumstances as determined by the principal. The parent/legal guardian must identify the nature of the unusual circumstances, and secure the school principal's written approval before the student is allowed to carry an electronic device on school property. Use of the device during the school day shall be restricted to the specific circumstances described. I understand that use of PED or other devices on District networks, including, but not limited to, the Internet is on an "as is" and "as available" basis.

Student Signature: _____
Student Name: _____
Date: _____

Parent/Guardian Signature: _____
Parent/Guardian Name: _____
Contact Number: _____
Date: _____
If 2. Applies, Please specify highly unusual circumstance (and the time period for which it shall be in effect) _____
_____
_____
_____

Physician Signature: _____
Physician Name: _____
Contact Number: _____
Date: _____
If 1. Applies, Please specify medical condition (and the time period for which it shall be in effect) _____
_____
_____
_____

Principal Signature: _____
Principal Name: _____
Date: _____

[8] Note that HIPAA Privacy Rules generally do not apply to K-12 schools because schools either (1) are not HIPAA covered entities or (2) are HIPAA covered entities but maintain health information only on students in records that are by definition "education records" under FERPA and, therefore, is not subject to the HIPAA Privacy Rule.