Instruction AR 6163.5

### Acceptable Use Regulations for Electronic Technologies

### I. PURPOSE

The purpose of this policy is to set forth guidelines for access to acceptable and safe use of the District's electronic technologies. Electronic technologies include but are not limited to computing devices and peripherals, printers, telephones, and the applications they support and/or access. The policy complements the District's Student Use of Technology Policy. BP /AR 6163.4

### II. GENERAL STATEMENT OF POLICY

The Salinas City Elementary School District provides technology resources to its students, staff, parents and community for educational, administrative, and informational purposes. The goal in providing these resources is to promote educational excellence in Salinas City Elementary schools by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers and support staff.

## III. EDUCATIONAL PURPOSE

Access to the technology in the Salinas City Elementary School District has been established for educational purposes. The use of the Salinas City Elementary School District's electronic technologies is a valued resource to our community. All electronic technologies must be used in support of the educational program of the District. This access may be revoked at any time for abusive or inappropriate conduct related to the use of electronic technologies.

School computers, telecom, memory devices, networks, and related hardware and software are the property of the Salinas City Elementary School District. At no time does the District relinquish its exclusive control of electronic technologies. Inappropriate use of District electronic technologies, including interfering with network functions and the standardization of technologies, may result in the limitation or revocation of access. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of electronic technologies may result in one or more of the following consequences: Suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate District policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under other applicable laws. Use of electronic technologies during the employee duty day should be restricted exclusively to educational purposes.

#### IV. DEFINITIONS

The term "users" refers to any person using the District's electronic technologies. The term "Internet" refers to an electronic communications network that connects computer networks and organizational computer facilities around the world. The term "intranet" refers to the District's network, which restricts access to authorized users, which may include students, staff, parents, contractors, vendors and volunteers. The term "electronic technologies" refers to, but is not limited to, computers and peripherals, printers, telephones, and the applications they support and/or access.

#### V. UNACCEPTABLE USES

Users are responsible for anything set on the network with their name or other individual identified, e.g., IP address, on it. Users shall not engage in any activity that disrupts or hinders the performance of the District's electronic technologies. Specifically, the following uses of the District's electronic technologies are considered unacceptable:

- A. Users will not use the District's electronic technologies to access, review, upload, download, store, print, post, receive, transmit or distribute:
  - 1. Pornographic, obscene or sexually explicit material or other visual depictions that are harmful to minors;
  - 2. Obscene, abusive, profane, lewd, vulgar, rude, inflammatory, libelous, threatening, disrespectful, or sexually explicit language;
  - 3. Materials that use language or images that are inappropriate in the educational setting or disruptive to the educational process;
  - 4. Information or materials that could cause damage or danger of disruption to the educational process;
  - 5. Materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination, or any other material that would violate any law.
  - Orders made by shopping online during time designated as off-limits by the District.
  - 7. Personal photos, files or music not related to educational purposes for any extended length of time.
- B. Users will not use the District's electronic technologies to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.
- C. Users will not use the District's electronic technologies to engage in any illegal act or violate any local, state or federal statute or law.
- D. Users will not use the District's electronic technologies for political campaigning.
- E. Users will not physically or electronically vandalize District technologies nor use the District's electronic technologies to vandalize, damage or disable the property of another person or organization.
  - 1. Users will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means.

2. Users will not tamper with, modify or change the District's electronic technologies software, hardware or wiring or take any action to violate the District's security systems.

- 3. Users will not use the District's electronic technologies in such a way as to disrupt the use of the system by other users.
- 4. Users may not add or remove any software nor modify the equipment, software configuration, or environment. All electronic technology requests must go through the District's Technology Department processes.
- F. Users will not use the District's electronic technologies to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.
- G. Users will not use the District's electronic technologies to post information in public access areas regarding private information about another person. Private information includes personal contact information about themselves or other persons, or other personally identifiable information including, but not limited to, addresses, telephone numbers, identification numbers, account numbers, access codes or passwords, labeled photographs or other information that would make the individual's identity easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message.
- H. Users will not engage in any behavior that can be considered cyberbullying. Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation.
- I. Users will not attempt to gain unauthorized access to the District's electronic technologies or any other system through the District's own electronic technologies or personal technologies. Users will not attempt to login through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user. Access through any means other than an individual's user login and password is not permitted and will be addressed by disciplinary means.
- J. Messages, files and records on the District's electronic technologies may not be encrypted without the permission of appropriate administrative school authorities. Users must keep all account information and passwords private. The District reserves the right to deploy any electronic means to encrypt District information and files on users' personal devices. The District also reserves the right to employ any electronic means to remove District information and District files on users' personal devices.

Instruction AR 6163.5

- K. Users will not use the District's electronic technologies in any way that may violate trademark copyright laws or usage licensing agreements:
  - 1. Users will not use another person's property without the person's prior approval or proper citation,
  - 2. Users will not load, download or exchange pirated software or copy software to or from any school computer including malware, free-ware and shareware;
  - 3. Users will not plagiarize works they find on the Internet or other information resources.
- L. Users will not use the District's electronic technologies for unauthorized commercial purposes or for financial gain unrelated to the Mission/Vision of the District. Users will not use the District's electronic technologies to offer or provide goods or services or for product advertisement, except as authorized by the District administration.
- M. The District does not support personal equipment. Individuals will not install any personal equipment or software on any district-owned systems without an approved "Application for Use of Personal Devices on School Premises" (Board Approved, Feb. 2013).

#### VI. FILTER

- A. With respect to any of its electronic devices with Internet access, the School District will monitor online activities of users and employ technology protection measures during any use of such devices by minors and adults. The technology protection measures utilized will use best efforts and industry standard approaches to block or filter Internet access to any visual depictions that are obscene, violent, child pornography, or harmful to minors and violate current CIPA, COPPA, FERPA and any other laws protecting minors online.
- B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:
  - 1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, violence, sex, or excretion; or
  - 2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
  - Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
- C. Access to chat rooms, social media, discussion boards, school-issued email and other forms of direct electronic communications are limited to applications approved by the District and/or hosted within the District domain for the safety and security of minors.

Instruction AR 6163.5

D. An administrator, supervisor or other person authorized by the Superintendent may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.

- E. The District is obligated to monitor and/or review filtering activities.
- F. The School District will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Administrative Regulation 6163.4- Student Use of Technology shall establish expectations for appropriate student conduct when using the Internet or other forms of electronic communication, including, but not limited to, prohibitions against:

- 1. Accessing, posting, submitting, publishing, or displaying harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs
- Intentionally uploading, downloading, or creating computer viruses and/or
  maliciously attempting to harm or destroy district equipment or materials or
  manipulate the data of any other user, including so-called "hacking"
- 3. Distributing personal identification information, including the name, address, telephone number, Social Security number, images, photos, or other personally identifiable information, of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person

The Superintendent or designee shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. 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 cyberbullying, and how to respond when subjected to cyberbullying.

### VII. TAKE HOME DEVICE PROCEDURES

All parents/guardians are expected to attend a parent meeting at the school site their child attends. All parents and students are required to sign a contract before being allowed to take the Chromebook home. If parent/guardian cannot attend the meeting, the School District will make available an alternate form of completing the requirements. All parents/guardians of transfer/new students will be required to complete the same requirements.

At the end of each school year, students will turn in their Chromebooks and power adapters. Failure to turn in the device will result in the student being charged the full replacement cost. Power supplies will be charged replacement costs as well. The breakdown of costs will be provided by the District. The District may also file a report of stolen property with the local law enforcement agency.

Students that transfer out of or withdraw from SCESD must turn in their device and power supplies to the school office before their last day of attendance. Failure to turn in the device will result in the student being charged the full replacement cost. The District may also file a report of stolen property with the local law enforcement agency.

Students are bound by the SCESD Acceptable Use Agreement, Administrative Procedures, Notice of Parental Rights policies, and all other student behavior guidelines wherever they use their devices. Similarly, the District actively uses an Internet content filter at both the ISP (Internet Service Provider) and the local level. Both are compliant with the Federal CIPA (Children's Internet Protection Act), COPPA (Children's Online Privacy Protection), and FERPA (Family Educational Rights and Privacy Act) laws and regulations. All devices, regardless of physical location (in or out of school), will have all Internet activity protected and monitored by the District.

## VIII. USAGE OF EQUIPMENT

Students may use devices at any time and in any building, classroom or setting unless a staff member has specifically prohibited the student(s) from using the device(s). Classroom teachers have the right to allow or disallow the use of devices during instructional or examination/assessment time, not otherwise specified on an educational plan. (Instructional time includes classroom time, assemblies, or any other time which is monitored by a teacher.)

No pupil shall be prohibited from possessing or using an electronic signaling device that is determined by a licensed physician and surgeon to be essential for the health of the pupil and use of which is limited to purposes related to the health of the pupil. If a student wishes to use an electronic communication device at an unauthorized time for medical purposes, his/her parent/guardian must submit a written request for permission to the school principal or designee to determine the validity of the request (Education Code 48901.5).

Examples of acceptable use of electronic devices include, but are not limited to:

- A Web search for classroom or related subject matter information.
- The use of any application (app) pertaining to, or related to, the current classroom subject such as but not limited to the use of any Google Apps for Education (GAFE) application.
- The reading of digital text or textbook on a device.
- Connecting through social media or a "back-channel" discussion or chat initiated by the classroom teacher.
- Asking appropriate questions of the teacher or others digitally through a learning management system or another platform.
- Collaborating on an assignment through
- Taking an assessment as instructed by the teacher.
- Taking notes on the subject being discussed.

Instruction AR 6163.5

Any accommodation made for a student on an Individual Education Plan (IEP) or a 504
 Plan.

When inappropriate or disruptive use of a student-operated electronic device is suspected, teachers should redirect the student behavior, as appropriate. All student behavior is subject to the rules in his/her school's Notice of Parental Rights.

Electronic devices are to be considered a tool that the student needs to accomplish his/her schoolwork during the day just like a textbook or a notebook. Confiscation of a device may adversely affect that student's ability to participate in other classes or simply put him/her at a disadvantage and prohibit the student from accessing the curriculum in other classes.

Examples of inappropriate or disruptive uses include but are not limited to:

- 1. Cheating or academic dishonesty. Students found in violation of academic honesty are subject to the consequences of cheating and plagiarism in his/her school's Notice of Parental Rights.
- Taking photos, recording video or audio of another person(s) (all persons including but not limited to students, teachers, substitute teachers, administrators) without gaining consent from that person(s) and unless it has been established beforehand as part of an assigned project and which will be monitored by a SCESD staff member. Furthermore, students should not post anything online of another person without prior consent, as per the teacher's direction; under district Notice of Parental Rights.
- 3. Taking pictures, recording audio or video in locker rooms or bathrooms.
- 4. Checking or responding to personal phone calls, emails, texts, social media applications, chats, messages etc. during class time.
- 5. Listening to music or watching a video without headphones or headsets (unless directed by the teacher). Headphones/headsets must be utilized in a manner in which is does not prevent a student from missing key instruction, curriculum or emergency announcements.

Any student who uses an electronic device in an unlawful manner or who unlawfully shares inappropriate material via phones, email, social media, or other electronic means may be subject to severe disciplinary action, including, but not limited to, out-of-school suspension, revocation of Device Take-Home agreement, daily check-out of electronic device for the remainder of the school year, and/or any other disciplinary action as deemed appropriate by school administration.

Devices are intended for use at school each day. In addition to teacher expectations for the device use, school messages, announcements, calendars, and schedules may be accessed using the device. Students must be responsible to bring their device to all classes, unless specifically instructed not to do so by their teacher.

#### **Devices Left at Home**

If students leave their device at home, they are responsible for getting the course work completed as if they had their device present.

If a student repeatedly (three or more times as determined by any staff member) leaves their device a home, they may be placed in the "Loaner" program—meaning they will check out a device in the morning and return it at the end of the school day (time to be determined by school). Students in the "Loaner" program will not take their device home.

Students may come off the "Loaner" program after period of time (set by the teacher o administrator), the device will be returned for student use at home. If this incident occurs again, the student may be referred to the school administrator.

If a student leaves their device at home for two consecutive days, they may be required to bring in the device and have a mandatory inspection of said device.

#### **Devices Undergoing Repair**

Loaner devices may be used by students when they leave their device for repair. Please note that there may be a delay in getting a device should the school not have enough to distribute.

<u>Loaner devices must remain at school as part of the "Loaner" program</u>— loaner devices will not be sent home with students.

Loaner devices will only be issued for use in school until all costs of replacement have been paid should there be any cost associated with repairs.

#### **Charging Your Device's Battery**

Devices must be brought to school each day in a fully charged condition. Students need to charge their devices each evening.

Repeat violators may be subject to disciplinary action and result in phone calls home and/or referrals to school administration.

In cases where use of the device has caused batteries to become discharged, students may be able to connect their device to a power outlet in class.

## Photo Library/Screensavers/Background photos

Inappropriate media should not be on the device and may not be used as a screensaver or background photo.

Presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drug, and gang-related symbols or imagery will result in disciplinary actions and may also result in a loss of device privileges.

Photos/videos require a large amount of storage space on the device. Only photos that are for an educational purpose should be saved to the device or Google Drive. All other photos/videos (not for an educational purpose) should not be taken or stored.

Instruction AR 6163.5

#### Sound, Music, Games, or Programs

Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes or the teacher allows for headphone/headset use.

Data Storage on the device is limited and should be managed by the students so that the full educational potential of the device is available. Data storage on Google Drive for Education is unlimited for all student and staff accounts.

Students may be directed by school personnel to remove pictures, music, videos if the storage of instructional materials is compromised.

Only music/sound files that are obtained legally for educational purposes are allowed.

#### **Printing**

Printing will not be available with the device.

#### **Home Internet Access**

Students do not need Internet access at home when accessing offline Google applications such as Docs, Sheets, Slides, or assignments in Google Classroom of this type.

Students are allowed to set up access to home wireless networks on the district devices. This may assist students with the ability to complete, retrieve, access, etc. educational content used in classes with the device successfully. It is not the responsibility of SCESD to assist students in accessing any network outside of the school environment.

To protect students, software is installed on the SCESD network, and on the student devices that will filter or block any content deemed inappropriate or harmful by SCESD. This includes but is not limited to child pornography as set out in CA. Code 18.2-374.1:1; obscenity as defined in CA. Code section 18.2-372; and non-educational social media or social networking spaces. The software will filter web content when the device is on or off of the SCESD network. Web content filters are not 100% accurate and sometimes allow access to content that should be blocked. If a teacher, parent, guardian, or student sees questionable content on a SCESD assigned device, they will need to contact school administration or the SCESD Technology Department immediately.

There may be times that the SCESD filter is not accessible outside of the network due to maintenance, or reasons beyond the control of the SCESD Technology Department. Should this happen, the student device will not be able to access the internet during that time.

### IX. PARENT'S RESPONSIBILITY FOR TAKE-HOME DEVICES

#### Parent/Guardian Responsibilities

Talk to your children about values and the standards that your children should follow on the use of the Internet just as you do on the use of all media information sources such as television, telephones, movies, and radio. Become increasingly active participants by asking your child/children to show you what sites they are navigating to and/or what apps are being used and how they work. The following resources will assist in promoting positive conversation(s) between you and your children regarding digital citizenship as it relates to Internet safety, conduct, and Netiquette:

Instruction AR 6163.5

- https://www.netsmartz.org/Home
- https://www.commonsensemedia.org/parent-concerns

Ensure that siblings and other family members are not using the device for their personal use. Also ensure that pets and younger siblings do not have access to the district device(s) so that the device is not damaged.

Parents are responsible for the general care of the device that has been issued by the school. Devices that are broken or fail to work properly must be taken to the school office as soon as possible so that they can be assessed by the SCESD Technology Dept.

If a device is turned in for assessment, the Technology Department will complete an Assessment Form that identifies the necessary repair(s) or replacement. A copy of the completed Assessment Form will be shared with the parent/guardian in order to determine next steps.

### **Device Damaged Accidentally**

Parents/Guardians may choose to purchase their own device insurance since accidental damage not covered under manufacturer's warranty. Parents are responsible for any and all damages.

#### X. LIMITED EXPECTATION OF PRIVACY

By authorizing use of the School District electronic technologies, the Salinas City Elementary School District does not relinquish control over content or data transmitted or stored on the network or contained in files. Users should expect only limited privacy in the contents of personal files on the District's electronic technologies.

- A. Routine maintenance and monitoring of the District's electronic technologies may lead to a discovery that a user has violated this policy, another School District policy, or the
- B. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or School District policy.
- C. Parents have the right at any time to investigate or review the contents of their child's files and e-mail files. Parents have the right to request the termination of their child's individual account at any time.
- D. District staff are advised that the School District retains the right at any time to investigate or review the contents of their files and e-mail files based upon legal complaints or specific allegations regarded as misuse of technologies. In addition, District staff are advised that data and other materials in files maintained on or transmitted through the District's electronic technologies may be subject to review, disclosure or discovery under the Minnesota Government Data Practices Act.
- E. The District will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with School District policies conducted through the District's electronic technologies.

#### XI. ELECTRONIC TECHNOLOGIES ACCEPTABLE USE AGREEMENT

- A. The proper use of the Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents and staff of the District.
- B. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a school account or resource to access the Internet.
- C. The SCESD Acceptable Use Agreement for students must be read and signed by the user and parents or guardians. Internet Use Agreement for employees must be signed by the employee. The form must then be filed with the District.
- D. All users shall be responsible for the protection and security of their passwords. Users shall have the ability to change passwords to maintain the confidentiality of logon codes.

#### XII. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the District's educational technologies is at the user's own risk and is provided on an "as is, as available" basis. The District will not be responsible for any damage users may suffer, including, but not limited to, loss, damage or unavailability of data stored on the District's systems or for delays or changes in or interruptions of service or mis-deliveries or non-deliveries of information or materials, regardless of the cause. The District is not responsible for the accuracy or quality of any advice or information obtained through or stored on the District's electronic technologies. The District will not be responsible for financial obligations arising through unauthorized use of the District's educational technologies or the Internet.

## XIII. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the District's electronic technologies must not violate other policies and regulations of the District, including but not limited to the District policies on Gifts and Donations Nondiscrimination, Harassment and Violence, Web site and Intranet, Instructional Materials Selection and Review, and Curriculum Goals.

#### XIV. USER NOTIFICATION

- A. All users shall be notified of the District policies relating to electronic technologies Acceptable Use Agreement.
- B. This notification shall include the following:
  - 1. Notification that Internet use is subject to compliance with District policies, and all applicable State and Federal laws.
  - 2. Disclaimers limiting the District's liability relative to:
    - a. Information stored on District systems including diskettes hard drives, or servers, CD, DVD, memory stick or similar devices, or any other media storage:

- b. Information retrieved through the District's computers, networks or online resources;
- Personal property used to access the District's computers, networks or online resources;
- d. Unauthorized financial obligations resulting from use of District resources/accounts to access the Internet.
- A description of the privacy rights and limitations of school sponsored/managed Internet accounts.
- 4. Notification of password ownership and password protection procedures.
- 5. Notification that, even though the District may use technical means to limit student Internet access, these limits are not impenetrable and are not the sole means of enforcing the provisions of this policy.
- 6. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student and/or the student's parents/guardians.
- 7. Notification that student email addresses may be provided to District-approved third-party providers for access to educational tools and content.
- 8. Notification that third-party vendors requesting access to student data must agree to, and sign, the district Student Data and Privacy Agreement (DPA)
- 9. Notification that the collection, creation, reception, maintenance and dissemination of data via the Internet, including electronic communications, is governed by School Board Policy 406, Public and Private Personnel Data, and School Board Policy 515, Protection and Privacy of Pupil Records.
- 10. Notification that, should the user violate the District's Acceptable Use Agreement, the user's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.
- 11. Notification that all provisions of the SCESD Acceptable Use Agreement are subordinate to local, state and federal laws.

# XV. PARENTS' RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

A. Outside-of-school, parents bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies and other possibly offensive media. Parents are responsible for monitoring their student's use of the District's educational technologies, including school-issued email accounts and of the Internet if the student is accessing the District's electronic technologies from home or through other remote location(s).

B. Parents will be notified that their students will be using District resources/accounts/school- issued email to access the Internet.

#### This notification should include:

- 1. A copy of the SCESD Acceptable Use Agreement provided to the student user;
- 2. A description of parent/guardian responsibilities;
- 3. A notification that the parents have the option to request alternative educational activities not requiring Internet access and the material to exercise this option;
- 4. A statement that the SCESD Acceptable Use Agreement must be signed by the user, parent or guardian, and the supervising teacher prior to use by the student; and
- 5. A statement that the District's Electronic Technologies Acceptable Use Agreement is available for parental review.

#### XVI. IMPLEMENTATION AND POLICY REVIEW

- A. The Superintendent, or designee, is directed to develop the necessary guidelines for the implementation of this policy. The Superintendent, or designee, may develop appropriate user notification forms, guidelines and procedures necessary to implement this policy for submission to the School Board for approval.
- B. The Superintendent, or designee, shall revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.
- C. The District's Internet policies and procedures are available for review by all parents, guardians, staff and members of the community.

Legal References: 17 U.S.C. § 101 et. seq. (Copyrights) 15 U.S.C. § 6501 et. seq. Children's Internet Protection Act of 2000 (CIPA) 47 U.S.C. § 254 47 C.F.R. § 54.520 (FCC rules implementing CIPA) Title III of the Elementary and Secondary Education Act of 1965, 2013