Educational Board-Approved Policies

A13*:* Digital Use Policy

Purpose:
Albert Einstein Academies provides technology to enhance student learning and support the instructional program. All students must use these resources safely and responsibly. The Superintendent or designee shall notify students and parents/guardians about authorized uses of technology, user obligations and responsibilities, and consequences for unauthorized use and/or unlawful activities per this Board policy and AEA's Acceptable Use Agreement.

This policy implements the Internet safety requirements of the Children's Internet Protection Act (CIPA) and the Protecting Children in the 21st Century Act to safeguard minors and ensure eligibility for Universal Service (E-rate) discounts on Internet access, telecommunications services, and other eligible products and services.

Resource Review:
Teachers, administrators, and/or library media specialists are expected to review the technological resources and online sites that will be used in the classroom or assigned to students in order to ensure that they are appropriate for the intended purpose and the age of the students. Under reasonable supervision of instructional staff and other authorized adults, students may use the Internet and online resources provided for educational purposes in the schools, programs, and facilities operated by AEA.

Definition of Technology:
AEA technology encompasses a broad range of devices and platforms, including computers, networks, emails, tablets, smartphones, wearable tech, and any other current or future innovations. This includes use on AEA-owned or personal devices both on and off the school premises.

Acceptable Use Agreement:
Before using AEA technology, students and their parents/guardians shall reference the Acceptable Use Agreement. In that agreement, the parent/guardian shall agree not to hold AEA or any AEA staff responsible for the failure of any technology protection measures or user mistakes or negligence and shall agree to indemnify and hold harmless AEA and AEA staff for any damages or costs incurred.

Configuration

AEA configures each Chromebook with the most recent version of Google Chrome that is compatible with all of AEA's applications and services. Students are not provided with administrative access to ensure AEA remains compliant with all county, state, and federal directives including the Children's Internet Protection Act. In addition, AEA configures all chromebooks to automatically and electronically provide software and hardware statistics, usage reports, and location reports.

Monitoring and Privacy:
The Superintendent or designee reserves the right to monitor, examine, and reasonably restrict system activities to ensure appropriate use of technological resources by students at any time without advance notice or consent. Electronic communications, Internet use, and downloaded material, including files deleted from a student's account under specific conditions, may be monitored or read by teachers and other employees. Students have no reasonable expectation of privacy in use of the AEA technology. In compliance with Federal Communications Commission rules for CIPA, a technology protection measure shall continuously filter Internet access in the schools and programs operated by AEA. Students are prohibited from using computers with Internet access where the technology protection measure is not enabled. ***A student's personally owned device may be searched in cases where there is a reasonable suspicion, based on specific and objective facts, that the search will uncover evidence of a violation of law, AEA policy, or school rules.***

The Superintendent or designee may gather and maintain information pertaining directly to school safety or student safety from the social media activity of any AEA student in accordance with EDC 49073.6 - Student Records.

Whenever a student is found to have violated AEA's Acceptable Use Agreement, the principal or designee may cancel or limit a student's user privileges or increase supervision of the student's use of the AEA's equipment and other technological resources, as appropriate. Inappropriate use also may result in disciplinary action and/or legal action in accordance with law and Board policy.

The Superintendent or designee, with input from students and appropriate staff, shall regularly review and update procedures to enhance the safety and security of students using AEA technology and to help ensure that AEA adapts to changing technologies and circumstances.

Reference: EDC 49073.6

Internet Safety

The Superintendent or designee shall ensure that all AEA computers with Internet access have a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced. (20 USC 6777; 47 USC 254; 47 CFR 54.520)

To reinforce these measures, the Superintendent or designee shall implement rules and procedures designed to restrict students' access to harmful or inappropriate matter on the Internet and to ensure that students do not engage in unauthorized or unlawful online activities.

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors. (Penal Code 313)

AEA's Acceptable Use Agreement 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

2. 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, or other personally identifiable information, of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person

4. Using electronic communication devices to video or voice record in any way or under any circumstances which infringe the privacy rights of other students, staff members or other persons.

STUDENT USE OF TECHNOLOGY (continued)

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 one's own personal identification 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.

Legal Reference:

EDUCATION CODE
49073.6 Student records; social media
51006 Computer education and resources
51007 Programs to strengthen technological skills
60044 Prohibited instructional materials
PENAL CODE
313 Harmful matter
502 Computer crimes, remedies
632 Eavesdropping on or recording confidential communications
653.2 Electronic communication devices, threats to safety

UNITED STATES CODE, TITLE 15
6501-6506 Children's Online Privacy Protection Act
UNITED STATES CODE, TITLE 20
6751-6777 Enhancing Education Through Technology Act, Title II, Part D, especially:
6777 Internet safety
UNITED STATES CODE, TITLE 47
254 Universal service discounts (E-rate)
CODE OF FEDERAL REGULATIONS, TITLE 16
312.1-312.12 Children's Online Privacy Protection Act
CODE OF FEDERAL REGULATIONS, TITLE 47
54.520 Internet safety policy and technology protection measures, E-rate discounts
COURT DECISIONS

BOARD APPROVED POLICY

Approved and Adopted: [date]

Albert Einstein Academies (AEA) Student Internet Acceptable Use

Students will have access to:

- Electronic mail (e-mail) communication with people all over the world.
- Information, online databases and news from a variety of sources and research institutions.
- AEA-provided software and public domain/shareware software of all types.
- Discussion groups on a wide-variety of topics.
- Variety of web-based and software programs to publish content to the web.
- Collaborative web-based programs for the purpose of project-based learning.
- Online courses and curriculum, academic software and electronic learning resources.
- Personal electronic communication devices (tablets, smart phones, MP3 players, etc.) to be used for a variety of educational purposes including but not limited to accessing the web.

Responsibilities

AEA has taken reasonable precautions to restrict access to "harmful matter" and to materials that do not support approved educational objectives. "Harmful matter" refers to material that, taken as a whole by the average person applying contemporary statewide standards, appeals to the prurient interest, and is matter which, taken as a whole, depicts or describes in a patently offensive way sexual conduct and which, taken as a whole, lacks serious literary, artistic, political or scientific value for minors. (Penal Code, section 313) The teacher and staff will choose resources on the Internet that are appropriate for classroom instruction and/or research for the needs, maturity, and ability of their students. AEA takes no responsibility for the accuracy or quality of information from Internet sources. Use of any information obtained through the Internet is at the user's risk. AEA is not responsible for lost or broken personal devices when they are used on AEA campus.

Acceptable Use

The purpose for our schools having access to the Internet is to enhance teaching and learning by providing access to 21st century tools and resources as well as online instruction. Use of another organization's data networks (e.g. Cell Phone Carriers) or computing resources must comply with rules of that network as well as AEA user policies.

Prohibited Uses

Transmission of any material or conducting an activity in violation of any federal or state law, and AEA policy is prohibited. This includes, but not limited to, the display or distribution of:

a. Bullying by using information and communication technologies (cyber-bullying);
b. Defamatory, inappropriate, abusive, obscene, profane, sexually oriented, threatening, racially offensive or illegal material. Downloading, viewing or sharing inappropriate content, including pornographic, defamatory or otherwise offensive material is prohibited;
c. Advertisements, solicitations, commercial ventures or political lobbying;
d. Information that encourages the use of controlled substances or the use of the system for the purpose of inciting crime;
e. Material that violates copyright laws.
f. Vandalism, unauthorized access, "hacking," or tampering with hardware or software, including introducing "viruses" or pirated software, is strictly prohibited (Penal Code, Section 502).

Warning: Inappropriate use may result in the cancellation of network privileges, discipline including but not limited to suspension and expulsion, and/or legal action in accordance with AEA policies/procedures.

Privileges

The use of the Internet is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. The administration, teachers and/or staff may request the site system administrator to deny, revoke or suspend specific user access.

Network Rules and Etiquette

The use of the Internet requires that students abide by AEA rules of network use and etiquette. These include, but not limited to, the following:

a. Be polite. Do not send abusive messages to anyone.
b. Use appropriate language. Anything pertaining to illegal activities is strictly forbidden.
Note: E-mail and web-based programs are not private and are subject to review by staff.

People who operate the system have access to all mail. Messages relating to, or in support of, illegal activities must be reported to appropriate authorities.
c. Maintain privacy. Do not reveal the personal address, phone numbers, personal web sites, images or other personal information of yourself or other persons. Before publishing a student's picture, first name, or work on the Internet, the school must have on file a parent release authorizing publication.
d. Cyber-bullying is considered harassment.
e. Respect copyrights. All communications and information accessible via the network are assumed to be the property of the author and should not be reused without their permission
f. Do not disrupt the network.
g. Do not create unauthorized wireless networks to access AEA's network. This includes establishing wireless access points, wireless routers and open networks on personal devices.
h. Do not use any software or proxy service to obscure either the student's IP address or the sites that the student visits.
i. Do not disable or bypass or attempt to disable or bypass any system monitoring, filtering or other security measures.
j. Do not access or attempt to access material or systems on the network that you are not authorized to access.
k. Do not install software on AEA equipment without the permission of a teacher or other authorized AEA staff person.

No Expectation of Privacy

There is no expectation of privacy in students' use of AEA technology. AEA reserves the right to access stored computer records and communications, files, and other data stored on AEA equipment or sent over AEA networks. Such communications, files, and data are not private and may be accessed during routine system maintenance; during inspection of AEA equipment at the end of the school year/term or agreed upon use period; and review of individual files or monitoring of individual activity when there is a reasonable suspicion that the student is engaging in an inappropriate use.

Cyber-Bullying

Cyber-bullying is the use of any electronic communication device to convey a message in any form (text, image, audio, or video) that intimidates, harasses, or is otherwise intended to harm, insult, or humiliate another in a deliberate, repeated, or hostile and unwarranted

manner. Staff and students will refrain from using personal communication devices or AEA technology to cyber-bully one another. Cyber-bullying may include but is not limited to: a. Spreading information or pictures to embarrass; b. Heated unequal argument online that includes making rude, insulting or vulgar remarks; c. Isolating an individual from his or her peer group; d. Using someone else's screen name and pretending to be that person; e. Forwarding information or pictures meant to be private.

Security

Security on any computer system is a high priority. Safeguard all personal passwords. Students should not share passwords with others and should change passwords frequently. Students are expected to notify an administrator immediately if they believe their student account has been compromised. Students shall not allow other students to use their account or use another student's account, with or without the account owner's authorization.

If you feel you can identify a security problem with the AEA network, please report this to the site network administrator or other administration, either in person, in writing, or via the network. Do not demonstrate the problem to other users. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the Internet.

Vandalism

Vandalism will result in cancellation of privileges and reimbursement for damages. This includes, but is not limited to, the uploading or creation of computer viruses.

Technology Equipment

All AEA students have access to student Chromebook. Student Chromebooks are assigned in each classroom to accommodate every learner. In the event a student requires to take a Chromebook home, a comparable device may be checked out from the front office. Students are advised to treat the equipment with care. Please reference the device loan agreement for further details.

Damaged or Stolen Equipment

If the loaned device is damaged or stolen, the student or parent/guardian is required to immediately notify AEA Academies or email support@aeacs.org. Students may not be issued a new device until the previous device is returned or recovered. Recovery costs

may be incurred if the device is damaged beyond repair or missing. The approximate cost of a replacement Chromebook is approximately $ _____.

Technology Equipment Asset Tags

AEA records the serial number, wireless media access control (Chromebook) address, and asset number of every technology device. The asset tag with the asset number is located on the back or rear of every device. The student is responsible for ensuring the asset tag remains on the equipment throughout the loan period. If the asset tag falls off or is removed, the student must notify AEA immediately as AEA may not be able to identify equipment without an asset tag. Equipment that cannot be identified using a serial number or asset tag cannot be accepted and the replacement fee must be paid.

Collection

If technology equipment is not returned by the end of the equipment loan period, AEA will make every attempt to recover the outstanding equipment. In the event that AEA is unable to recover outstanding technology equipment through conventional means, AEA reserves the right to file a police report for stolen property with the San Diego Police Department naming the student and the student's Parent or Guardian. If a student willfully damages AEA's property, including but not limited to AEA's technology, equipment and networks, or fails to return AEA's property that has been loaned to the student, the student's parents/guardians are liable for all damages caused by the student's misconduct. AEA may withhold the student's grades or transcripts until the damages have been paid or the property has been returned. If the student and the student's parent/guardian are unable to pay for the damages or to return the property, AEA will provide a program of voluntary work for the minor in lieu of the payment of monetary damages. Upon completion of the voluntary work, the student's grades and transcripts will be released. A student over the age of majority shall be liable for the same. (Ed. Code § 48904).

Technical Issues

AEA provides technical support to Students for all technical issues. Students can receive support by sending an email to support@aeacs.org. Students are not permitted to perform or authorize repairs on any AEA technology equipment.

Digital Services and Initiatives

AEA username and ID:

Students are provided with an AEA username and ID by AEA. The AEA username and ID is the student's access point for all digital services and initiatives. AEA may adjust the naming convention for students with special circumstances or in the case of a duplicated username and ID.

Digital Accounts

Students are provided with a Google and Powerschool account. The account allows the student to access the entirety of the Workspace collection of products including Gmail, Classroom, Drive, Docs, Sheets, Hangouts, Keep, Calendar, and more. For more information about G Suite for Education on Google's website:https://edu.google.com/products/productivity-tools/. Students are also provided with a Powerschool account which is our Student Information System. Students may access state assessments, grades, attendance records and educational records through this portal.

Separation through Graduation

Graduated students of AEA are granted the privilege of maintaining portions of their AEA username and ID. This includes access to their G Suite (Google) account. AEA is not required to assist or support Graduated Students with issues related to their AEA username and ID or associated services. All portions of the Digital Use Policy apply while the Graduated students AEA username and ID is active.

Content Ownership

AEA retains the right to use, without restrictions, royalties, or further permission, all content, materials, and schoolwork created using AEA provided equipment and services. Content may be used in published or digital marketing materials, communications, and AEA owned websites. In some instances, AEA also reserves the right to retain ownership of all content, materials, and schoolwork created using AEA provided equipment and services.

Digital Citizenship

The student agrees to abide by the generally accepted rules of digital citizenship conduct in a responsible, ethical and polite manner while using any AEA technology/resources.

This means that you will not use AEA technology to post, view, or share negative or damaging content about yourself or others.

Additionally, you agree to avoid social media sites that contain negative or defamatory messages about yourself or others.

Failure to practice good digital citizenship will result in the following restorative practices and progressive Consequences:

- Warning 1: Verbal warning and restorative circle between the student and teacher and/or any other staff member(s) who observed the violation.
- Note that depending on the severity of the issue, students may also be suspended and expelled.
- Warning 2: Phone call home and restorative circle between student, teacher, and administration. A written warning will be issued at this point. Note that depending on the severity of the issue, students may also be suspended and/or expelled.
- Warning 3: Continued student's choice to not practice good digital citizenship will lead to parent/principal designee meeting and possible removal of Chromebook privileges.

Copyright Infringement

Copyright law protects the value of creative work. Copyright infringement happens when you inappropriately copy someone else's work that is protected by copyright. When you make unauthorized copies of someone's creative work, you are taking something of value from the owner without the person's permission. Federal law provides severe civil and criminal penalties for the unauthorized reproduction, distribution, rental or digital transmission of copyrighted music, movies and other material. If you are unsure of whether something can be legally copied or not, you must request permission to copy from the copyright holder. You and/or your parents
are responsible for any copyright penalties that you incur while using any AEA technology or device. You agree to abide by all patent, trademark, trade name, and copyright laws.

Limitation of Liability

AEA shall not be responsible for any damages suffered by the scholar, including those arising from service interruptions, unauthorized use, loss of data, damage and/or exposure

to potentially harmful or inappropriate material or people. Use of any information obtained via the Internet or communications technologies is at the student's own risk. AEA specifically denies any responsibility for the accuracy or quality of information obtained through the Internet.

AEA assumes no liability for personal technology, including but not limited to computers, smartphones, network access laptops, or other electronic signaling laptops, if such laptops are damaged, lost or stolen. The student and the student's parent and/or guardian shall indemnify and hold AEA harmless from any losses sustained or any other claims as the result of use or misuse of the technology resources provided for by AEA for use by the scholar, and/or the loss or damage of personally-owned technology.

Seizure

School personnel may confiscate student-owned Electronic Communication Devices (ECDs) when they have reasonable cause to believe that ECDs have been used to bully or harass other students or employees of AEA, or use of ECDs will materially and substantially disrupt school activities. AEA employees shall store confiscated ECDs in accordance with the following:

1. Each school site shall designate a specific drawer or cabinet in the main office where confiscated items can be securely locked and stored.

2. Access to the keys to the above-referenced drawer or cabinet shall be limited to one or two persons only. The keys shall not be maintained in public view.

3. The school site shall maintain a log in the locked drawer or cabinet indicating the date and time an item was confiscated, by whom, the name of the student whose property was confiscated, a description of the item, and when it was retrieved. The parent or guardian retrieving the item must print their name, relationship, date and time of retrieval, and sign the log indicating receipt of the property.