ACCEPTABLE USE AGREEMENT

The use of any district technology shall constitute agreement to the terms and conditions outlined by this policy.

Parents and students will be notified of this policy annually, in conjunction with the Parent-Student Handbook. Understanding of and agreement to all rules, policies and laws must be acknowledged on the Acceptable Use Agreement portion of the Receipt of Annual Parent-Student Handbook by signature of both student and parent/guardian.

The following uses of AUHSD technology are unacceptable and in violation of this policy:

1. Uses that violate any state or federal law or municipal ordinance
2. Selling or purchasing any illegal substance
3. Threatening, harassing or making defamatory or false statements about others - cyberbullying is prohibited by state law
4. Accessing, transmitting or downloading offensive, harassing or disparaging materials
5. Using any district computer to pursue hacking, internal or external to the district or attempting to access information that is protected by privacy laws
6. Using the district Internet system to engage in any unlawful act including, but not limited to, arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, espionage, or threatening the safety of any person
7. Accessing, transmitting or downloading computer malware (including viruses, worms, spyware, adware, Trojan horses) or other harmful files or programs or in any way degrading or disrupting any computer system performance
8. Accessing, transmitting or downloading child pornography, obscene depictions, harmful materials or materials that encourage others to violate the law, materials that advocate participation in hate groups or other potentially dangerous groups.
9. Transmitting or downloading confidential information, copyrighted materials, unauthorized software, or committing plagiarism
10. Obtaining and/or using an anonymous e-mail site
11. Obtaining and/or using an anonymous proxy site
12. Accessing another user's e-mail without their permission; deleting, copying, modifying or forging other user's e-mails, files or data
13. Unauthorized use of another user's password
14. Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes"
15. Selling, advertising or buying anything over the Internet for personal financial gain
16. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for political purposes or soliciting votes
17. Using any district computer contrary to Social Media section of this policy
18. Using games or game sites for non-educational purposes
19. Gambling or engaging in any other activity in violation of local, state or federal law

20. Streaming video or audio content for purposes other than legitimate AUHSD business and / or educational purposes

INTERNET SAFETY: USER OBLIGATIONS AND RESPONSIBILITIES

Users are authorized to use the district's equipment to access the Internet or online sites/services in accordance with user obligations and responsibilities specified below and in accordance with Board of Trustees' policies.

The district's technology system shall be used only for purposes related to education. Commercial, political and/or personal use unrelated to an educational purpose is strictly prohibited.

1. Users shall not access, post, submit, publish or display harmful or inappropriate matter that is threatening, obscene, disruptive or sexually explicit, or that can be construed as harassment or disparagement of others based on their race/ethnicity, national origin, gender, sexual orientation, age, disability, religion or political beliefs.

2. Users shall not disclose, use or disseminate personal identification information about themselves or others when using electronic mail, chat rooms, or other forms of direct electronic communication. Students are also cautioned not to disclose such information by other means to individuals located through the Internet without permission of their parents/guardians. Personal information includes the student's name, address, telephone number, Social Security number, or other individually identifiable information.

3. Users shall not use the system to encourage the use of drugs, alcohol or tobacco, nor shall they promote unethical practices or any activity prohibited by law or district policy.

4. Copyrighted material may not be placed on the system without the author's permission. Users may download approved copyrighted material for their own use only.

5. The act of 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, destroy, steal or wastefully misuse district equipment or materials or the data of any other user.

6. Users who engage in activities commonly described as "hacking" (i.e., the unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of the district, a business, or any other governmental agency obtained through unauthorized means) are subject to district discipline and loss of privileges.

7. Users shall not post anonymous messages, read other users' mail or files, they shall not attempt to interfere with other users' ability to send or receive electronic mail, nor shall they attempt to delete, copy, modify or forge other users' mail or intellectual

property.

8. Users shall report any security problem or misuse of the services to the teacher, principal or appropriate administrator.

The administrator, principal or designee shall make all decisions regarding whether or not a user has violated Board Policies. The decision of the administrator, Principal or designee shall be final.

Inappropriate use shall result in cancellation of the user's privileges, disciplinary action and/or legal action in accordance with law and Board Policy.

GUIDELINES FOR REMOTE ACCESS DEVICES

The following security guidelines attempt to ensure that confidential information that is used or accessed from off-campus is protected to the same degree that it is protected when accessed via a district workstation. All students who use a remote access device to access district networks must follow these guidelines. A remote access device is any device, district or personally owned that can connect to a district network. Devices may include, but are not limited to, cellular telephones, personal digital assistants (PDA), tablet computers, sub-notebook computers, notebook computers, laptop computers, and personal computers.

- Students and vendors using remote access devices are responsible for any loss, damage or wear to the remote access device if the equipment is provided by district.
- Students and vendors are responsible for taking precautions so that only authorized individuals can gain access to any district information that is stored or accessed from their remote access device.
- Students and vendor agrees that the use of the equipment, software, data and supplies provided by the department is limited to authorized persons If the equipment is provided by district,
- Students and vendors must take the necessary precautions ensuring that unauthorized individuals cannot view confidential information that appears on the screen when using the remote access device.
- Students and vendors shall never share their passwords with anyone.
- Students and vendors agree to abide by software licensing and security agreements.
- A current version of antivirus software, with up-to-date virus definitions, must be installed on the remote access device. Students and vendors are responsible for making sure the antivirus software and signature files are kept current on the remote access device they are using.
- Anti-spyware software is required for all relevant remote access devices.
- A local firewall is required for all relevant remote access devices

GUIDELINES FOR PERSONALLY OWNED DEVICES

The use of personal mobile devices, such as laptops, cellular phones, tablets, pagers, or other electronic signaling devices, by students on campus is subject to all applicable District policies and regulations concerning technology use, as well as the following rules and understandings:

- The District accepts no financial responsibility for damage, loss or theft. Devices should not be left unattended.
- The District reserves the right to delete district-owned data from personal devices in the event of the loss of a device, termination, graduation, any separation from the District, or any other appropriate event. The District will try not to access or erase personal items.
- The District will monitor all Internet or intranet access.
- District staff is not responsible for and will not repair personally-owned devices.
- If the District has reasonable cause to believe that the student has used the device to violate the law or District policy, the device may be searched by authorized personnel and/or law enforcement may be contacted.
- Permission to have a student mobile device at school is contingent on parent/guardian permission in the form of a signed copy of the District's Information Technology Acceptable Use Agreement.
- Students will comply with policies herein and will affirm compliance during network onboarding process.
- All costs for data plans and fees associated with mobile devices are the responsibility of the student. The District does not require the use of personal mobile devices and does not rely on personal devices in its instructional program or extracurricular activities.
- Use during class time must be authorized by the teacher.
- Personally-owned devices that are authorized for use on campus must operate quietly, may not obstruct the view or passage of others, must operate on its own power, and may not have distracting lights or districting moving parts.
- Use of devices on campus during the school day, while attending school-sponsored activities, or while under the supervision and control of a school district employee must be specifically authorized by school policy or procedure.
- The district acknowledges the importance of electronic communication between students and parents, particularly in school-wide emergency situations and recognizes the importance of electronic devices as tools for 21st century learning environments. The intent of this policy is to authorize the use of electronic devices for legitimate educational purposes unless the use of the devices causes a disruption or interferes with the orderly operation of the school environment. Misuse or use inconsistent with school policy will subject student to disciplinary consequences.
- Students may not take, possess or share obscene photographs or video.
- Students may not photograph, videotape or otherwise record any instructional materials, including tests.

GUIDELINES FOR DISTRICT- OWNED MOBILE DEVICES

When a student is using a District-owned mobile device, all of the guidelines related to personally-owned mobile devices apply in addition to the following:

- The device may be used only for school-related purposes.
- Users may not download applications to the device without permission from the teacher or other District employee.
- Users must follow all user agreements associated with the applications.
- The student and parent/guardian will be responsible for the replacement cost if the device is lost or is damaged because of intentional misuse.

E-MAIL

Electronic mail (e-mail) is available to most students. It is a valuable tool in improving communication within and outside of AUHSD. The system belongs to AUHSD and is to be used for educational purposes. There should be no expectation of privacy in anything created, stored, sent, or received on the e-mail system. To ensure compliance and proper usage, the following regulations have been established.

A. Basic Guidelines
   1. All e-mail messages, as all paper documents, are the property of the District and are subject to office policy, procedures, and control.
   2. E-mail is for school use. Messages can be stored, forwarded and printed. As such, the Department has the right to review them. The messages become public documents available to the public and subject to court subpoena in any legal proceedings.
   3. Correspondence via e-mail should comply with all the same requirements for correspondence prepared by staff as identified in the AUHSD Procedures and Policies Style Guide.
   4. Include a pertinent subject title.
   5. Messages should be brief and concise.
   6. E-mail messages should not contain profanity, racial or sexual slurs, or other unprofessional language.
   7. E-mail messages should include professional fonts, colors, backgrounds, logos, etc.
   8. Personal information which falls under any applicable privacy regulation shall not be communicated through or attached to e-mail, unless such information is necessary in the course of business and has a legitimate purpose. Communication of personal information must be considered as “confidential” at all times for the protection of individual privacy rights. Unauthorized access to personal information is prohibited. Specific examples of personal information includes, but is not limited to, the following:
      a. Social security numbers
      b. Employee’s salary, address or telephone number
      c. Disciplinary action or documentation or performance problems
      d. Details of a health or medical condition

9. Mailbox space should be kept to a minimum. Delete unneeded messages.
10. Outlook data files, including, but not limited to: PST, are not permitted.
11. Students are responsible for any messages sent using their e-mail account.
12. E-mail messages automatically include the Anaheim Union High School District Disclaimer indicating that if the individual is not the intended recipient of the message, any reproduction contained in the transmission is strictly prohibited unless it is subject to review by AUHSD.

    ANAHEIM UNION HIGH SCHOOL DISTRICT E-MAIL DISCLAIMER
    This communication and any documents, files, or previous e-mail messages attached to it, constitute an electronic communication within the scope of the Electronic Communication Privacy Act, 18 USCA 2510.
    This communication may contain non-public, confidential, or legally privileged information intended for the sole use of the designated recipient(s). The unlawful interception, use or disclosure of such information is strictly prohibited under 18 USCA 2511 and any applicable laws.
13. Students shall exclusively use their AUHSD-provided email account when using email to communicate with AUHSD teachers and staff.

B. Passwords
   1. Students are responsible for their passwords on their e-mail account.
   2. Each user is expected to change the password from the generic password to a personalized password and keep it secure – including not sharing passwords with other parties. Continued use of the generic password can result in someone else sending messages in the owner's name, in which case the owner is held responsible. Automatic logging onto e-mail should NOT be used.
   3. Passwords should be created with the following:
      a. Use BOTH upper- and lower-case letters. It is preferable to use upper case letters on any character but the first character.
      b. Place numbers and punctuation marks randomly in your password.
      c. Make your password long and complex, so it is hard to crack. Between 8 to 20 characters long is recommended.
      d. Use one or more of these special characters: ! @# $ % * ()-= ,
      e. Spaces are not allowed
      f. Make your password easy to type quickly. This will make it harder for someone looking over your shoulder to steal it.

E-Mail Retention

E-Mail messages, created or received in the transaction of AUHSD business, are public records and is open to public inspection. Depending on the content and topic of a particular message, it may or may not be exempt from public inspection under the California Public Records Act.

The e-mail system will retain e-mails for a reasonable time frame for both disaster recovery and the recently amended federal legislation. Currently, deleted e-mails will be removed from the users' inbox after 7 days, and sent items 365 days; however, the user will be able to retrieve the e-mail from the archive server for a period of 5 years.

SOCIAL NETWORKING

Access to Social Networking Sites

A student with a educationally-related need to access a social networking site using AUHSD Technology may request such access from his/her school administrator, or designee.

CONSEQUENCES

Any student violation of board policy should be treated as a Class II infraction. Disciplinary consequences can range from warning, conference, confiscation, detention, alternatives to suspension or suspension. Each school may develop their own progressive discipline based on local school site decisions. The consequences for violating this policy include, but are not limited to, one or more of the following:

- Suspension of district network privileges**,**
- Revocation of network privileges,
- Suspension of Internet access,
- Revocation of Internet access,
- Suspension of computer access,
- Revocation of computer access,
- School suspension,
- Expulsion,
- Referral to legal authorities for prosecution under California Penal Code Section 502.

At the beginning of each school year, parents/guardians shall be notified of the district's policy and administrative regulations regarding access by students to the Internet and online sites/services and the permitted use of electronic devices (either District owned or personally owned) on campus. (Education Code 48980)

The principal or designee shall oversee the maintenance of each school's technology and may establish guidelines and limits on their use. He/she shall ensure that all students using these resources receive training in their proper and appropriate use.

March 28, 1996
Revised: October 2001
Revised: January 2005
Revised December 2005
Revised January 2012
Revised October 2014
E