March, 2023

INFORMATION TECHNOLOGY ACCEPTABLE USE AGREEMENT

Please read the following carefully. This is a legally binding agreement and must be signed before you will be given an access account.

The Anaheim Union High School District (AUHSD) supports instruction through the use of educational and administrative computers, school-licensed software and other media, as well as networks and servers. The AUHSD provides Internet access through an electronic network. The Internet is an electronic highway connecting millions of computers and billions of people all over the world. Students, teachers, support staff, parents and School Board members with accounts on the Internet server have limited access to:

1. Electronic mail (e-mail) communication with people all over the world
2. Information and news from a variety of sources and research institutions
3. Cloud-based applications
4. Discussion groups on a wide variety of educational topics
5. Access to many university libraries, the Library of Congress and more.

With access to computers and people all over the world comes the availability of some material that may not be considered to be of educational value within the context of the school setting. The AUHSD has taken precautions to restrict access to controversial materials. However, on a global network, such as the Internet, it is impossible to control the content of all available materials.

Following are guidelines provided to establish the responsibilities of everyone using AUHSD computers, media, computer networks and/or Internet access.

AUHSD network accounts are a privilege. If a user violates any of these provisions, his or her access may be terminated and any future access could be denied.

TERMS AND CONDITIONS

I. ACCEPTABLE USE: The purpose of AUHSD networks is to support instruction, research, and the business of conducting education by providing access to unique resources and opportunities for collaborative work. The use of an account must be in support of education consistent with the educational objectives of the AUHSD system. Additionally, use of other organizations' networks or computing resources must comply with rules appropriate to that network. Transmission of any material in violation of any United States or state law or state agency provisions is prohibited. This includes, but is not limited to: Copyrighted material, threatening or obscene material, material protected by trade secret, or commitment of plagiarism. Use for any non-educational purpose (as defined by the Anaheim Union High School District) or commercial activity by any individual or organization, regardless of status, is not acceptable. Use for product advertisement or political lobbying is strictly prohibited.

AUHSD must be notified of a request for a tablet, laptop, personal or District, or any other device to be used with network connectivity. The request must be submitted prior to the beginning of the class/meeting taking place.

For guest speakers, requests should be made by the class instructor/supervisor/director on their behalf prior to the class/meeting. School sites should direct their requests to the Technology Services Technician; the District office should contact the Education and Information Technology Department (EIT). All equipment must be examined by the Technology Services Technician or EIT before connecting to the AUHSD networks. All AUHSD computers/

laptops/tablets must be updated by the Technology Services Technician or EIT three times during each year.

All software to be installed on District computers must be licensed. Installation will be performed by the Technology Services Technician or EIT staff.

Students and employees should be aware, that before a request to use a personal device can be considered, the following conditions for a tablet, laptop, PC or other smart device must be met:

1. The operating system of the laptop / computer must be current with the latest patches and updates for that version (available at www. microsoft.com / www.apple.com). If these patches are not current at the time the laptop/PC is brought in for use, the request for network access will be denied. Critical updates shall also be applied to ChromeOS and Android devices.

2. Anti-virus software must be installed on the laptop / computer and virus definitions must be current. A recent scan on the laptop / computer by this software should also have been completed. If these patches are not current at the time the laptop / computer is brought in for use, the request for network access will be denied. AUHSD is unable to assist with these types of updates or services. No District-owned software shall be installed on personally owned computers.

3. District staff is not responsible for and will not repair personally-owned devices.

4. Use of device must follow all protocols and guidelines put forth that explicitly or implicitly relates to use of said device in the AUHSD network and / or on one of the District sites.

II. PRIVILEGES: The use of AUHSD network accounts is a PRIVILEGE, not a right; therefore, inappropriate use may result in a cancellation of those privileges. AUHSD administration and the System Administrator(s) (SA) will deem what is inappropriate use. The decision of the AUHSD administration or the SA is final. The SA may close an account at any time. Based on the recommendation of teachers and staff, the administration of the AUHSD may request that the SA deny, revoke, or suspend specific user accounts.

The District will make every effort to protect students and staff from access to inappropriate materials by strict monitoring at the classroom level and through restrictions implemented by hardware, software, and Internet filters which will monitor network activity. The Board of Trustees recognizes it is impossible to eliminate access to all controversial materials. Furthermore, because of the need for monitoring activity there can be no expectation of privacy when using District technology (AUHSD Board Policies 6209 and 7901.03). Any attempt to gain access to inappropriate or controversial materials shall be grounds for revocation of access to District technology and may result in other disciplinary action. (AUHSD Board Policies 6209 and 7901.03)

III. NETIQUETTE (NETWORK ETIQUETTE) and PROTOCOLS: The use of an account on any AUHSD network requires that you abide by accepted rules of network etiquette which include, but are not limited to, the following:

1. ***BE COURTEOUS AND RESPECTFUL.*** System users are expected to be polite. System users may not send abusive, insulting, harassing, discriminatory, inflammatory, or threatening messages to others. You will promptly disclose to your teacher or administrator a message you receive that is inappropriate or makes you feel uncomfortable. You should not delete such messages until instructed to do so by an appropriate staff member.
2. ***USE APPROPRIATE LANGUAGE.*** System users are expected to use appropriate language; vulgarities or obscenities, libelous or other inappropriate references will not be tolerated.
3. ***APPROPRIATE ACTIVITIES***. Anything pertaining to illegal activities is strictly forbidden. Any activity not directly related to the educational mission of the District is strictly forbidden. Activities relating to, or in support of, illegal activities will be reported to the appropriate authorities. If you mistakenly access inappropriate material, you should immediately report this access to a teacher or administrator. This will protect you against a claim that you have intentionally violated this policy.
4. ***PRIVACY.*** Do not reveal the full name, personal address, phone numbers or other personal information of yourself or any persons. All communications and information accessible via the network should be assumed public property. Electronic mail is not guaranteed to be private. Systems Administrators have access to all mail. Messages relating to, or in support of, illegal activities will be reported to the appropriate authorities.
5. ***CONNECTIVITY***. Do not use the network in such a way that would limit or disrupt the use of the network by others.
6. ***SERVICES.*** AUHSD will not be responsible for any damages suffered. This includes loss of data resulting from delays, non-deliveries, or service interruptions caused by negligence, errors or omissions. Use of any

information obtained via the networks is at the user's risk. AUHSD specifically denies any responsibility for the accuracy or quality of information obtained through its network services.

7. ***SECURITY***. Security on any computer system is a high priority. If users can identify a security problem on any of the networks, they must notify a System Administrator, either in person or via the network, as soon as possible. Users must not demonstrate the problem to other users. Use of network service accounts provided by the AUHSD is not transferable or assignable. Any users who knowingly allow another to use the account assigned to them will immediately lose their access privileges and may be subject to further disciplinary and/or legal action. Attempts to fraudulently log in on any network as a System Administrator or another user will result in immediate cancellation of user privileges and the user may be subject to further disciplinary and/or legal action. Any user identified as a security risk, or having a history of problems with other computer systems, may be denied access to the networks and other computer services.

8. ***CYBERBULLYING.*** The District believes every child is entitled to a safe school environment free from discrimination and bullying. Consistent with state and federal law, the District prohibits bullying and discrimination and provides a timely and effective complaint procedure for pupils who believe they have been the victim of bullying or discrimination. The District also is mindful that, at times, behavior that is rude or insensitive may nevertheless be constitutionally protected in the context of a public-school environment. Such conduct can best be combatted and prevented with effective strategies that involve pupils, parents and school employees in collaborative efforts to teach tolerance and ensure equal educational opportunities for all. (Board Policy 8701.01)

9. ***USER ACCOUNTS AND PASSWORDS.*** You are responsible for your individual account(s) and should take all precautions to prevent others from being able to access your account(s). Under no condition should you provide your password to another person nor post it in your work area. Staff network passwords are required to be changed annually.

10. ***VANDALISM AND ELECTRONIC MISCHIEF***. Vandalism will result in cancellation of privileges and disciplinary action. This includes, but is not limited to, electronic mischief, electronic theft, the uploading or creation of computer viruses, attempts to tamper with any programs, applications, files, etc.

11. ***UPDATES***. AUHSD may occasionally require new registration and account information from users to continue providing services. Users must notify the System Administrator(s) of any changes in account information.

12. ***E-MAIL ABUSE POLICY (SPAM)*.** Spam is harmful because of its negative impact on public attitudes and also because it can overload the network and resources. Employees will be held liable for such infringement even if the spamming action was done by a third party for the students' benefit (i.e., if a student does the spamming, the teacher or supervising staff member may also be held responsible).

13. ***AUHSD WEBSITES.*** All rules and guidelines herein apply to student, staff and department web pages as well as any system pages such as those stored in learning management systems, student information systems, G-Suite and Office 365.

IV. UNACCEPTABLE USES OF THE COMPUTER NETWORK OR INTERNET

Unacceptable uses include, but are not limited to, the following:

1. Uses that violate any state or federal law, municipal ordinance, Board Policy, administrative regulation, or district practice.
2. Selling or purchasing any illegal substance.
3. Threatening, intimidating, 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, committing plagiarism, license, trademark, patent, or other intellectual property rights.
10. Obtaining and/or using an anonymous e-mail site.
11. Obtaining and/or using an anonymous proxy site and/or any VPN software.
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, crypto-mining, 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.
21. Disclose or in any way cause to be disclosed confidential or sensitive district, employee, or student information without prior authorization from a supervisor

V. Student Devices

The use of tablets, laptops, cellular phones, or electronic signaling devices (DEVICES) by students on campus is prohibited during normal school hours, unless such use is part of the instructional program and is authorized by the District. Devices it must remain off unapproved times, and must be stored in a locker, backpack, purse, pocket or other place where it is not visible during school hours.

If such a DEVICE is observed or heard at unapproved times by school staff, it will be confiscated until redeemed by a parent or guardian. Repeated violations of this policy may result in discipline. If the device rings or is visible during testing, it will be confiscated and the student removed from the test situation. Exceptions to this policy may be granted by the site administrator for purposes relating to the health needs of a student.

Photographing, videotaping or otherwise recording individuals without their permission is strictly prohibited.

DEVICES may be used on campus at approved times. Students in high school grades 9-12 may use cell phones during the lunch period. The District is not responsible for lost or stolen DEVICES. Due to the time required, the District will not investigate lost or stolen devices. Their security is the sole responsibility of the student.

VI. Student Email

AUHSD has provided Gmail accounts for all students. The account serves as a vital link to many instructional resources. You may opt your student out of this email account by contacting the registrar at your student's school.

Your signature on this document is legally binding and indicates you have read the Terms and Conditions carefully and understand their significance. Any user who violates the terms of this policy will immediately lose his/her access privilege and may be subject to disciplinary and/or legal action.

Your signature below indicates your agreement with the terms and conditions listed above.

_____	_____	_____
PRINT NAME	SIGN NAME	DATE