The Board of Trustees intends that technological resources provided by the district be used in a responsible and proper manner in support of the instructional program and for the advancement of student learning.

It is the purpose of this policy to outline acceptable staff behavior with respect to the use of electronic information resources and district technology.

DEFINITION

District technology includes, but is not limited, computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, cloud-based applications, infrastructure and data, email, USB drives, wireless access points, switches, ~~tablet~~ computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

PRIVILEGES

The use of district technology is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges. The use of district technology is a privilege permitted at the district's discretion and is subject to the conditions and restrictions set forth in applicable Board policies and administrative regulations. The Board of Trustees authorizes district and school network administrators to suspend or revoke access to district technology when questionable conditions arise.

PERSONAL RESPONSIBILITY

The Superintendent or designee shall notify employees about authorized uses of district computers and consequences for unauthorized use and/or unlawful activities.

Employees are expected to maintain consistently high levels of personal responsibility regarding the use of district technology. Employees are expected to use district technology safely, responsibly, and primarily for work-related purposes. Rules found in the Education Code 48900, employee handbooks, and this policy clearly apply to employees conducting electronic research and communications. Additionally, the Board of Trustees expects that all system users will observe the definitions and authorized procedures described in Penal Code Section 502.

One fundamental need for acceptable employee use of district technology is respect for, and protection of, password/account code security, as well as restricted databases, files and other data. Personal passwords/accounts shall be created to protect employees utilizing electronic resources to conduct research. Employees shall not gain unauthorized access to the files or equipment of others, access electronic resources by using another person's name or electronic identification, or send anonymous electronic

communications. Furthermore, employees shall not attempt to access any data, documents, emails, or programs in the district's system for which they do not have authorization.

NO EXPECTATION OF PRIVACY

Employees shall have no expectation of privacy in any message, file, data, document, facsimile, or any other form of information accessed, transmitted to, received from, or stored on any technology owned, leased, used, maintained, moderated or otherwise operated by AUHSD, including, but not limited to, e-mails and other electronic communications. During the course of carrying out their responsibilities, authorized AUHSD personnel or other authorized representatives may access any technology, including employee e-mails and other electronic communications without the knowledge of the user. AUHSD also has software and systems in place that monitor and record all internet / intranet and e-mail usage. AUHSD may capture user activity such as network resource and file access, data created, stored or transmitted in any form, telephone numbers dialed and web sites visited. Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Employees should be aware that, in most instances, their use of district technology (such as web searches or emails) cannot be erased or deleted.

All passwords created for or used on any district technology are the sole property of the district. The creation or use of a password by an employee on district technology does not create a reasonable expectation of privacy.

Employees are advised that employee e-mails and other electronic communications pertaining to the business of AUHSD generally are deemed to be public records and must be disclosed to members of the public upon request unless the records are specifically exempt from disclosure under the California Public Records Act. Moreover, documents may be subject to disclosure by subpoena or other legal process.

RECORDS

Any electronically stored information generated or received by an employee which constitutes a district or student record shall be classified, retained, and destroyed in accordance with BP/AR 5703 - District Records, BP/AR 81502 - Student Records, or other applicable policies and regulations addressing the retention of district or student records.

REPORTING

If an employee becomes aware of any security problem (such as any compromise of the confidentiality of any login or account information) or misuse of district technology, he/she shall immediately report such information to the Superintendent or designee.

CONFIDENTIALITY OBLIGATIONS

AUHSD endeavors to maintain the confidentiality of its internal e-mail systems and other electronically stored information, and employees are expected to respect that confidentiality. Employees shall not copy, move, or otherwise transfer confidential or sensitive information or data to a directory or storage location that does not have adequate access restrictions.

AUHSD websites available to the general public must contain a Privacy Statement.

To safeguard and protect the proprietary, confidential and sensitive business information of AUHSD and to ensure that the use of all technology is consistent with AUHSD legitimate business and educational interests, authorized representatives of AUHSD may monitor the use of technology, messages and files.

Users who become aware of a possible security breach involving AUHSD technology or data shall immediately notify the Chief Technology Officer or designee.

GUIDELINES FOR ONLINE SERVICES/INTERNET ACCESS

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that blocks or filters Internet access to visual depictions of obscenity, child pornography, or are harmful to minors, and that the operation of such measures is enforced. (20 USC 7001, 47 USC 254)

The Board desires to protect employees from access to harmful matter on the Internet and other online services. The Superintendent or designee shall implement rules and procedures designed to restrict employees' access to harmful or inappropriate matter on the Internet. He/she also shall establish regulations to address the safety and security of employees when using electronic mail, chat rooms and other forms of direct electronic communication.

Disclosure, use and dissemination of personal identification information regarding students are prohibited.

Staff shall supervise students while they are using online services and may ask teacher aides to assist in this supervision.

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.

Cyberbullying is an act that may be committed face-to-face or “by an electronic act.” An

"electronic act" is defined as "transmission of a communication, including but not necessarily limited to, a message, text, sound, or image, or a post on a social network Internet Web site, by means of an electronic device, including but not necessarily limited to, a telephone, wireless telephone or other wireless communication device, computer, or pager."

Technology is an important aspect to the district's objective to creative effective school to home parent communication to increase parent awareness and involvement. The district has implemented a variety of tools to facilitate parent communication including, but not limited to, a school-to-home telephony system, district and school web sites, and a student information system with parent and student portals that maintain pertinent student demographic and performance data. Employees are encouraged to populate these systems with appropriate and relevant data that make these systems useful.

It is expected that the use of district technology be limited to curriculum, instructional, and administrative projects by staff.

ACCEPTABLE USE

The use of Anaheim Union High School District's technology is a privilege which may be revoked at any time. Behaviors which shall result in revocation of access shall include, but will not be limited to: Damage to or theft of system hardware or software; alteration of system software; placement of unlawful information, computer viruses or harmful programs on or through the computer system, either public or private files or messages; entry into restricted information on systems or network files in violation of password/account code restrictions; and/or use of the network for personal gain or to engage in political lobbying.

The District will make every effort to protect staff from access to inappropriate material by monitoring 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.

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.

In order to help ensure that the district adapts to changing technologies and circumstances, the Superintendent or designee shall regularly review this policy, the accompanying administrative regulation and other procedures. He/she shall also monitor the district's filtering software to help ensure its effectiveness.

Access to electronic mail (e-mail) is a privilege and is designed to assist employees in the acquisition of knowledge and in efficiently communicating with others. The district e- mail system is designed solely for educational and work-related purposes. E-mail files are subject to review by district and school personnel.

Employees 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.

Employees are not permitted to obtain, download, view or otherwise gain access to materials which may be deemed unlawful, harmful, abusive, obscene, pornographic, descriptive of destructive devices, or otherwise objectionable under current district policy or legal definitions.

The district or school staff reserves the right to remove files, limit or deny access, and refer staff for violating the Board Policy for other disciplinary action. The Board of Trustees authorizes district and school administrators to monitor and review all aspects of the use of district technology.

INTELLECTUAL PROPERTY

Board Policy 7902 addresses the issues of copyright law. Users should assume that any material they did not create is copyrighted. Employees may not claim personal copyright privileges over files, data or materials developed in the scope of their employment. Although it is possible to download a wide variety of material, students and staff shall not create or maintain archival copies of these materials unless the source indicates that the materials are in the public domain.

SERVICES

While the district is providing access to electronic resources, it makes no warranties, whether expressed or implied, for these services. The district will not be responsible for the accuracy of information obtained through district technology or for any damages suffered by any person while using these services. These damages include loss of data as result of delays, non-delivery or service interruptions caused by district technology or the user's errors or omissions. The use or distribution of any information that is obtained through district technology is at the user's own risk. In addition, the district is not responsible for financial obligations arising from unauthorized use of the system.

SECURITY

The Board of Trustees recognizes that district technology security is an extremely high priority. The accounts and passwords provided to each user are intended for the exclusive use of that person. Any problems which arise from the user's sharing his/her password/account are the responsibility of the account holder. Any misuse may result in the suspension or revocation of account privileges. The use of an account by someone other than the registered holder will be grounds for loss of access privileges to district technology.

Users are required to report immediately any abnormality in the system as soon as they

observe it. Abnormalities should be reported to the classroom teacher and/or network administrator.

VANDALISM OF THE ELECTRONIC NETWORK OR TECHNOLOGY SYSTEM

Vandalism is defined as any malicious attempt to alter, harm or destroy equipment or data of another user, the district administrative network, or the other networks that are accessible via district technology. This includes, but is not limited to, the uploading or the creation of computer viruses, the alteration of data, or the theft of restricted information. Any vandalism of the district electronic network or technology system will result in the immediate loss of computer service, disciplinary action and, as appropriate, referral to law enforcement officials.

Cross References:

AUHSD Board Policies: 7902 Reproduction and Use of Copyrighted Materials
8700 Student Discipline
8708 Sexual Harassment, Students

Legal References:

Education Code: 48900 Suspension and expulsion
48980 Required notification at beginning of term

51006 Computer education and resources
51007 Programs to strengthen technological skills
51870-74 Education technology
51870.5 Student Internet access
60044 Prohibited instructional materials

Penal Code:
313 Harmful matter
502 Computer crimes, remedies
632 Eavesdropping on/or recording confidential communications
United States Code, Title 20:
6801-7005 Technology for Education Act of 1994
7001 Internet safety policy and technology protection measures, Title III funds
United States Code, Title 47:
254 Universal service discounts (E-rate)
Code of Federal Regulations, Title 16
312.2-312.12 Children's online privacy protection
Code of Federal Regulations, Title 47
54.520 Internet safety policy and technology protection measures, E-rate discounts
California Public Records Act
Federal Civil Procedure (2006 amendment)
AB 746

Board of Trustees
March 28, 1996
Revised: October 2001
Revised: January 2005
Revised: December 2005
Revised: January 2012
Revised: October 2014
Revised: January 2023
Revised: January 2025
E