Azusa Unified School District

ACCEPTABLE USE AGREEMENT

TERMS AND CONDITIONS FOR USE OF TECHNOLOGY RESOURCES PURSUANT TO BOARD POLICY 4040(a)

The Board of Education of the Azusa Unified School District recognizes that technological resources can enhance employee performance by offering effective tools to assist in providing a quality instructional program, facilitating communications with parents/guardians, students, and the community, supporting district and school operations, and improving access to and exchange of information. Responsible and appropriate use of technology is essential to productive work and educational environments.

This Acceptable Use Agreement ("Agreement") sets forth the rules and regulations that all District employees must follow. Each user of the District's computer resources agrees to the conditions established herein. It is the responsibility of every computer user to know these rules and regulations and to conduct activities accordingly.

SECTION 1.
PREAMBLE

I have read and understand this section _____
initial

The Azusa Unified School District's ("District") computer resources are provided subject to the rules and regulations set forth in this Agreement.

All users of District computer resources must sign this Agreement. Use of District computer resources in violation of this Agreement is prohibited.

SECTION 2.
DEFINITION OF TERMS

I have read and understand this section _____
initial

Computer resources: The sum total of all computers, workstations, mainframes, software, cabling, switchers, routers, servers, peripherals, networks, accounts, passwords, ID numbers, student information systems, and any and all data, equipment, or electronic devices owned or leased by the District including, but not limited to, District laptops and mobile communication devices, such as cellular telephones, pagers, personal digital assistants (PDAs), smartphones and mobile data devices.

System administrator: A person employed by District whose responsibilities include system or network administration. A system administrator performs functions including, but not limited to, installing hardware and software, managing computer networks, and keeping computers operational and investigating violations of the Agreement.

User: Someone who does not have system administrator responsibilities for a computer system or network but who makes use of that computer system or network. A user is still responsible for his or her use of the computer.

SECTION 3.
COVERAGE

I have read and understand this section _____
initial

Section 3.1 Access

District is committed to providing access to computer resources to all current employees consistent with the education and service missions of District.

Section 3.2 Privileges

Users do not own accounts on District computers. District owns the accounts and grants users the privilege of using the accounts. Computer files and electronic communications, including, but not limited to, email and voice mail, are not private.

Section 3.3 Responsibilities

As a condition of maintaining the privilege of using District computer resources, each user will be held responsible for his or her own actions which affect such resources. By signing the Agreement, each user acknowledges and agrees to abide by the terms of the Agreement. A user who violates the terms of the Agreement will be subject to revocation or suspension of the privilege of using the computer resources and may be subject to appropriate discipline.

3.3.1 District computer resources are to be used for District-related business, instruction, learning, and administrative activities. Use of District computer resources to engage in personal communications is not permitted, except in an emergency or incidental use, as defined in Section 4.2.2.

3.3.2 Users shall not attempt to modify any system or network or attempt to "crash" or "hack" into District systems. Users shall not tamper with any software protections or restrictions placed on computer applications or files. Unless properly authorized, users shall not attempt to access restricted portions of any operating system or security software. Users shall not attempt to remove existing software or add their own personal software to District computers and systems unless authorized.

3.3.3 Users shall use only their own designated computer accounts. Users are required to keep all user ID's, passwords, and account information confidential, and shall take reasonable precautions to prevent others from obtaining this information. Accounts are not transferable, and users shall not allow others to use their accounts.

Users shall respect the privacy and personal rights of others, and are prohibited from accessing or copying another user's e-mail, data, or other files without the prior express consent of that user.

3.3.4 Users are responsible for using software and electronic materials in accordance with copyright and licensing restrictions. The copying of software that has not been placed in the public domain is expressly prohibited by the Agreement.

3.3.5 No Expectation of Privacy: District computer resources and all user accounts are the property of District. There is no right to privacy in the use of the computer resources or user accounts, including, but not limited to, emails and voicemails. There is no right to privacy in personal technology devices which are used in accordance with Section 4.1.4 below.

In addition, users are hereby put on notice as to the lack of privacy afforded by electronic data storage and electronic mail in general, and must apply appropriate security to protect private and confidential information from unintended disclosure. Electronic data, including, but not limited to, e-mail, which is transmitted through District computer resources is more analogous to an open postcard than to a letter in a sealed envelope. Under such conditions, the transfer of information which is intended to be confidential should not be sent through District computer resources.

District reserves the right to monitor and access information contained on its computer resources and on personal technology devices which are used in accordance with Section 4.1.4 below under various circumstances including, but not limited to, the following circumstances:

3.3.5.1 Under the California Public Records Act ("CPRA"), electronic files are treated in the same way as paper files. Public documents are subject to inspection through CPRA. In responding to a request for information under the CPRA, District may access and provide such data without the knowledge or consent of the user.

3.3.5.2 District will cooperate with any local, state, or federal officials investigating an alleged crime committed by any person who accesses District computer resources, and may release information to such officials without the knowledge or consent of the user.

3.3.5.3 The contents of electronic messages may be viewed by a system administrator in the course of routine maintenance, or by the system administrator, Superintendent or designee(s) as needed for District administrative purposes, including investigation of possible violations of the Agreement or other District policies, and monitoring of on-line activities of minor students.

3.3.5.4 Electronic mail systems store messages in files. These files are copied to back-up devices in the course of system backups. The contents of these files and the copies on system backup tapes are subject to disclosure as stated in the preceding paragraphs.

3.3.5.5 Should the possibility of litigation arise, any electronically stored information may be preserved, reviewed and/or produced to appropriate people at the District's discretion including District personnel, attorneys, consultants, experts, and/or the court in connection with litigation or potential litigation.

3.3.5.6 Any electronically stored information may be preserved pursuant to a litigation hold, document retention or destruction policy or in connection with any appropriate law or regulation.

3.3.6 Receipt of Offensive Material: Due to the open and decentralized design of the Internet and networked computer systems, users are warned that they may occasionally receive materials which may be offensive to them. Users should report all such occurrences to the system administrator.

Section 3.4 Ethical Standards

All users must abide by ethical standards of on-line behavior that assure equitable, effective and efficient access and use of computer resources. Such ethical standards include, but are not limited to:

3.4.1 Honesty:

3.4.1.1 Users agree to represent themselves according to their true and accurate identities in all electronic messages, files and transactions at all times.

3.4.1.2 While using District computer resources, users agree to act within District standards of conduct including the prohibition on plagiarism.

3.4.2 Respecting Rights of Others:

3.4.3 Communicating in the same manner as is expected in the classroom or in the office (e.g., users should not use profanity and vulgarity in personal communication). Users shall not use District computer resources in any unlawful manner including, but not limited to, attempting to defraud another person or entity, threatening harm to another person, procuring or distributing obscene material in any form, or unlawfully harassing another person:

3.4.3.1 For purposes of the Agreement, "obscenity" or "obscene" means words, images or sounds which a reasonable person, applying contemporary community standards, when considering the contents as a whole, would conclude that they appeal to prurient sexual/physical interests or violently subordinating behavior rather than an intellectual or communicative purpose, and materials that, taken as a whole regarding their content and their particular usage or application, lack any redeeming literary, scientific, political, artistic or social value.

"Harassing" or "harass" means to engage in a knowing and willful course of conduct directed at another person which seriously alarms, annoys or harasses another person, and which serves no legitimate purpose. In addition, "Harassment" also means subjecting another person to unwelcome sexual advances, requests for sexual favors, and other verbal, visual or physical conduct of a sexual nature as set forth in California Education Code section 212.5.

3.4.4 Users shall respect the integrity and content of electronic documents or records issued or posted on-line by employees or students.

3.4.5 Users shall have respect for the access and security procedures and systems established to ensure the security, integrity and operational functionality of District computer resources.

Section 3.5 Disclosure of Personal Information

Employees shall not disclose confidential student information through use of computer resources in a manner which violates either the California pupil privacy laws (Ed. Code § 49060 et. seq.) or the Federal Education Rights Privacy Act ("FERPA") (20 U.S.C. § 1232g)

.

SECTION 4.
APPROPRIATE AND INAPPROPRIATE USES

I have read and understand this section _____ **initial**

District computer resources exist to support the instructional, cultural, research, professional and administrative activities of District community. In general, the same guidelines that apply to the use of all District facilities apply to the use of District computer resources. All users are required to behave in a responsible, ethical and legal manner as defined by the Agreement, and other existing District policies and regulations. The following sections define appropriate and inappropriate use of District computer resources:

Section 4.1 Appropriate Use

Activities deemed to be appropriate uses of District computer resources include the following:

4.1.1 Instructional use

4.1.1.1 Classroom instruction.

4.1.1.2 Research connected to academic and instructional concerns and interests.

4.1.1.3 Communication with colleagues and professional organizations and institutions if such communications are related to District educational programs and activities.

4.1.2 Administrative/Non-instructional use

4.1.2.1 District administrative and business communications and transactions.

4.1.2.2 Communication with colleagues and professional organizations and institutions if such communications are related to the operation of District.

4.1.2.3 Research connected with District concerns and interests.

4.1.3 Request to unblock Internet site access by District employees

In the event that a District employee has a legitimate and job-related need to access material which is otherwise prohibited by the Agreement or cannot be accessed because of restrictions placed on the material by an Internet blocking or filtering measure, such employee may submit a written request to the system administrator or designee requesting permission to access specific sites for the purpose of completing such job-related tasks or research.

4.1.4 Personal Technology Use

District recognizes that the use of certain technology devices, such as memory sticks, which are not owned by the District may be beneficial to District employees. Memory sticks and similar storage devices may be used with District computer resources if the user has current security software installed on all non-District equipment on which the memory stick or other storage device is used. Other than memory sticks and similar storage devices, District employees may not use laptops, PDAs, internet tablets, or other personal computing or mobile communication devices not owned or leased by the District with District computer resources which are connected to the District network, absent current security installed software and express written permission by the system administrator or immediate supervisor. Notwithstanding the above, employees may, without written permission by the system administrator, connect personal technology devices such as VCR/DVD players, document cameras, video or still cameras, mp3 players, AM/FM tuners/amplifiers to District equipment, such as projectors and televisions which are not connected to the District network, if there is a legitimate instructional or administrative purpose behind such use.

District employees may only use personal communication devices for personal purposes during nonduty times of the workday or for brief conversations. Instructional time may not be interrupted by a personal cellular telephone or mobile communication device, except in an emergency. Such activities shall not interfere with the work efficiency or performance of the employee and shall not interfere with the rights or work efficiency or performance of others.

4.1.5 Websites

Employees shall not develop any classroom or work-related websites, blogs, forums, or similar online communications representing the District or using District equipment or resources without written permission of the Superintendent or designee. Any such website, blog, forum, or similar online communications shall include a disclaimer that the District is not responsible for the content.

Section 4.2 Inappropriate Use

Use of District computer resources for purposes other than those identified in Section 4.1 is not permitted. Users who violate this section of the Agreement by engaging in inappropriate use of District computer resources will be subject to restriction, suspension, or revocation of user privileges and may be subject to discipline and criminal or civil sanctions if permitted by law. Users are specifically prohibited from using District computer resources in any manner identified in this section.

4.2.1 Displaying, viewing, downloading, sending or otherwise accessing material that is obscene, pornographic, or harmful to minors. The District will utilize Internet filtering and/or blocking measures to attempt to prevent user access to such materials.

4.2.2 Using District computer resources for personal purposes, other than incidental personal uses which do not interfere with an employee's work responsibilities, as determined by the Superintendent or designee. Incidental uses do not include any use that is prohibited under this Agreement. The District retains the right to limit or prohibit incidental uses at the discretion of the District's Superintendent or designee.

4.2.3 Destroying or damaging equipment, software, or data belonging to District or others.

4.2.4 Disrupting or unauthorized use of District accounts, access codes, or ID numbers.

4.2.5 Using District computer resources in ways which intentionally or unintentionally impede the computing activities of others are prohibited. Such activities include, but are not limited to: disrupting another person's use of computer resources by game playing, sending an excessive number of messages or e-mail, making or printing excessive copies of documents, files, data, or programs, introducing computer viruses onto District computer resources, or impersonating any person or entity under a false or unauthorized name.

4.2.6 Using District computer resources to violate copyrights, trademarks, and/or license agreements.

4.2.7 Using District computer resources to violate another person's privacy including, but not limited to, obtaining, accessing, distributing, or using another user's account, ID number, password, electronic files, data, e-mail, or confidential personal information.

4.2.8 Using District computer resources in an effort to violate District's academic policies.

4.2.9 Transmitting any advertising or promotional materials or engaging in commercial activity which is unrelated to District business including, but not limited to, buying, selling, advertising, or viewing property or services posted on ebay, Craigslist, Amazon, or other commercial websites.

4.2.10 Copying system files, utilities and applications that expressly belong to District without authorization.

4.2.11 Sending or storing messages and/or materials with the intent to defraud, harass, intimidate, defame, threaten, unlawfully discriminate, or otherwise violating the District's ethical standards under Section 3.4.

4.2.12 Inappropriate mass mailing, "spamming," or "mail bombing." Mass mailings directed to "All District Employees" or to any large subgroup of District employees shall be approved by the sender's immediate supervisor.

4.2.13 Disabling, tampering with, hacking or trying to break into any software protections or restrictions placed on computer applications or files.

4.2.14 Knowingly or carelessly introducing any invasive or destructive programs (e.g., spyware, viruses or worms) into District computer resources.

4.2.15 Attempting to circumvent local or network system security measures.

4.2.16 Installing unauthorized software programs on District computers or network systems and/or using such programs.

4.2.17 Ignoring or disobeying policies and procedures established for specific computer labs or network systems.

4.2.18 Using District computer resources for any activities which violate or are inconsistent with District policy or regulations.

SECTION 5.
VIOLATIONS: REPORTING AND CONSEQUENCES

I have read and understand this section _____
initial

Section 5.1 Employee Violations

Users shall report any suspected violation of the Agreement by a District employee to the employee's supervisor who shall immediately refer the matter to the system administrator and Superintendent for review. The Superintendent or designee shall then determine whether a violation of the Agreement has occurred. If the Superintendent or designee determines that a violation has occurred, he or she may take immediate action to restrict, suspend, or revoke the user's privileges. The user may also be subject to appropriate discipline.

SIGNATURE

I have read the District's Acceptable Use Agreement and understand its provisions. I accept responsibility for the appropriate use of District computer resources. I understand that use of computer resources in violation of the Agreement may result in the revocation or restriction of user privileges and appropriate discipline. I agree to report any use which is in violation of the Agreement to the system administrator or appropriate employee supervisor.

_____	_____	_____
Employee [PRINT NAME]	Signature	Date

cc: Personnel File