Acceptable Use Policy

Adelanto Elementary School District (AESD) recognizes that access to technology at school gives students more significant opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping our students develop 21st-century technology and communication skills. We provide access to various technologies for students and staff to meet this commitment. These technologies range from classroom to take-home devices to empower students to maximize their full potential and prepare them for successful futures.

AESD provides a wide range of technology resources for student use within the classroom and at home. Student devices are to be used solely for educational purposes. This Acceptable Use Policy (AUP) outlines appropriate use and prohibited activities. AESD expects every student to follow the rules and conditions listed in this document and any directions or guidelines given by AESD teachers, substitutes, administrators, and staff.

Mandatory Review

This AUP outlines the guidelines and behaviors that all users must follow when using District technology resources. Students must review this agreement each school year to educate themselves on expectations for responsible use of the AESD computer network. Additionally, employees supervising students who use the AESD computer network shall provide training on appropriate use. All District students and parents/legal guardians shall acknowledge receipt and understanding of this Agreement and agree in an electronic form to comply with the same.

Technologies Covered

The District may provide technological resources for student use, including Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, chat, and e-mail. The policies this document outlines are intended to cover all available technologies, not just those specifically listed.

General Policies

- The AESD network is intended solely for educational purposes or district business. The term "educational purpose" includes, but is not limited to, classroom activities, career development, and high-quality self-discovery activities.

- The AESD computer network has been established for educational purposes, not as a public access service or public forum. Adelanto Elementary School District has the right to place reasonable restrictions on material accessed or posted throughout the network.
- A content filtering solution is in place to prevent access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the Children's Internet Protection Act (CIPA). This includes all District devices taken off our computer network.
- This Agreement also pertains to users who connect via non-District network services (e.g., cell phones, mobile hotspots, etc.) while on District property or participating in school-related functions. However, AESD cannot be held responsible for content accessed through such services.
- Students must sign and adhere to this Agreement; parent/guardian permission is required for all students. The District is not responsible for the actions of students who violate this Agreement.
- The District reserves the right to monitor all activity on the AESD computer network and District-provided devices off our computer network. Students have no expectation of privacy concerning the usage of the computer network, even if the use is for personal purposes.
- In addition to this Agreement, students are expected to follow all aspects of the Student Use of Technology Policy (BP 6163.4) and Student Use of Technology Administrative Regulation (AR 6163.4). The same rules, good manners, guidelines, and laws used in daily school activities also apply to students using the AESD computer network.

Digital Citizenship Expectations

While utilizing any portion of the AESD computer network and equipment, students are expected to exhibit responsible behavior and avoid engaging in inappropriate use. The AESD computer network is considered a limited forum. Therefore, the District may restrict a student's use of the network for valid reasons, including but not limited to violations of the following:

- Students shall not post information that, if acted upon, could cause damage or danger of disruption to the educational environment for staff and/or students.
- Students shall not engage in electronic personal attacks that violate District policy or State or Federal law.
- Students shall not harass, bully, or engage in any activities intended to harm (physically or emotionally) another person. Harassment is persistently acting in a manner that distresses or annoys another person and includes, but is not limited to, online impersonation, intimidation, or denigration; sending persistent and unsolicited messages; cyber-stalking; and changing or manipulating the digital property of others.

- Students shall not distribute or post fabricated, harmful, or defamatory information about a person or organization.
- Students shall not use the AESD computer network, equipment, or personal devices to engage in criminal activity.
- Students shall not display, access, or send offensive, explicit, or inappropriate messages or content.
- Students shall not offer, provide, or purchase products or services through the AESD computer network.
- Students shall not use the AESD computer network for political lobbying.

Internet and Student Websites

- Access to Web-based resources is intended for educational purposes. Students are expected to adhere to the responsible use of guidelines as specified in this Agreement and District policy. Immediately report inappropriate sites to District staff.
- The use of any photographs or student work on any web pages must follow District guidelines.
- Material (graphics, text, sound, etc.) placed on any web pages are expected to meet academic standards of proper spelling, grammar, mechanics, the accuracy of the information, and legal copyright standards.
- All student webpages must have a link back to the homepage of the classroom, school, or district, as appropriate.

Electronic Communication

- Students may have access to programs that allow email, messaging, chat, social networking, etc. These accounts are to be used for specific educational purposes or activities by State and Federal law when on campus.
- Students shall not establish or access personal accounts through the District network for non-educational purposes.
- Students shall not repost content, including but not limited to pictures, messages, or videos, that were sent to them privately. Sender's permission as well as any subjects depicted in the content, and, in some cases, the parent/legal guardian is required for the reposting of content.
- Students shall not post private and/or personal information about another person, including, but not limited to, contact or identifier information.

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

Personal Safety

- Students shall not share personal contact and/or identifier information about themselves or others. Personal contact/identifier information includes but is not limited to address, telephone, school address, email address, or Social Security Number.
- Students shall not disclose personal contact information except to educational institutes for educational purposes, companies, or other entities for career development purposes, or without specific authorization.
- Students shall not agree to meet with someone they have met online.
- Students shall promptly disclose to a teacher or other school employee any message received that is inappropriate or makes the student feel uncomfortable.

Care of Equipment

- Students must take care of the technology-focused equipment, which can be considered a privilege.
- Users may not remove network cables, keyboards, or other components.
- Students may not modify the configuration or content of software installed on any District technology.
- Damages to technology may result in a charge being placed on the user's account.
- The District reserves the right to monitor, inspect, copy, and review district-owned devices

System Security

- Students are responsible for their accounts and should take all reasonable precautions to prevent others from using them, including, but not limited to, keeping passwords private.
- Students shall immediately notify a teacher or other school employee if they have identified a possible security problem. Students should not look for security problems because this may be considered an illegal attempt to gain access.

- Students shall not attempt to gain unauthorized access to any portion of the AESD computer network. This includes attempting to log in through another person's account or accessing another person's folders, work, or files. These actions are illegal, even if only for "browsing."
- Students shall not attempt to access non-student District systems.
- Students shall not deliberately attempt to disrupt the AESD computer network or destroy data by spreading computer viruses or other means. These actions are illegal.
- Students shall not intentionally attempt to access websites blocked by District policy, including proxy services, VPN, software, or websites.
- Students shall not use sniffing or remote access technology to monitor the network or other user's activity.

Software and Files

- Software is available to students to be used as an educational resource. Students shall not install, upload or download the software without District permission. Any software that disrupts the AESD computer network will be removed.
- Files stored on the AESD computer network are treated in the same manner as other school records. Routing maintenance and monitoring of the AESD computer network by authorized employees may lead to the discovery that a student has violated this Agreement or the law. Students should not expect that files stored on District servers or accessed through the AESD computer network are private.

Technology Hardware

- Hardware and peripherals are provided as tools for student use for educational purposes. Students are not permitted to install or relocate network hardware and/or peripherals (except for portable devices) or to modify settings to equipment without the consent of the District Information Technology Department.
- Students shall not connect unauthorized wired or wireless devices to the AESD computer network.

Vandalism

- Any malicious attempt to harm or destroy data, the network, or other network components connected to the network backbone, hardware, or software may result in the cancellation of network privileges. Appropriate disciplinary action will be taken.

Plagiarism and Copyright Infringement

- Students may access copyrighted material for educational purposes.
- All students are expected to follow existing copyright laws. Posting any material (graphics, text, sound, etc.) that violates federal or state law is prohibited. This includes but is not limited to, confidential information, copyrighted material, threatening or obscene material, and computer viruses.
- Copyrighted material shall not be placed on any system without the author's permission. Permission may be specified in the document, on the system, or must be obtained directly from the author.
- Students shall not plagiarize works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original works. This includes using Artificial Intelligence language models (e.g., ChatGPT).
- Students shall appropriately cite materials referenced or used in producing original work.

Videoconferencing/Classroom Video Feed

- All video conferencing must be for educational purposes.
- Students shall not record or stream classroom or other school-related activities without proper authorization. All such recordings or streaming must comply with student privacy laws.

Due Process

- The District's authorized representatives will cooperate fully with local, state, or federal officials in any investigation of illegal activities conducted through the AESD computer network.
- Disciplinary actions will be tailored to meet specific concerns related to the violation. Violations of this Agreement may result in a loss of access and other disciplinary and/or legal action.

Limitation of Liability

- The District makes no guarantee that the functions or the services provided by or through the AESD computer network will be error-free or without defects. The District will not be responsible for any damage suffered, including but not limited to loss of data, damage to personal devices, or service interruptions.

- The District is not responsible for the accuracy or quality of the information obtained through or stored on the AESD computer network. The District will not be liable for financial obligations arising through the unauthorized use of the network.
- The District utilizes a content filtering solution to block access to objectionable and inappropriate material on the Internet. However, preventing all such access is impossible, and a risk exists that a student may access material intended only for adults, even with filtering in place. No safeguard is foolproof, and the District is not responsible for material encountered on its computer network which may be deemed objectionable to a user or their parent/legal guardian.

Violations of This Agreement

Violations of this Agreement may result in loss of access and other disciplinary and/or legal action. Students' breach of this Agreement shall be subject to the consequences as indicated within this Agreement as well as other appropriate disciplinary action(s), including but not limited to:

- Use of AESD computer network only under direct supervision
- Suspension of network privileges
- Revocation of network privileges
- Suspension of computer privileges
- Suspension from school
- Expulsion from school
- Legal action and prosecution by the authorities

Federal and State Laws Related to Cybercrimes

Below are examples, but not an exhaustive list, of online conduct that may constitute a violation of federal and state laws relating to cybercrimes:

- **Criminal Acts:** These include, but are not limited to, "hacking" or attempting to access computer systems without authorization, threatening/harassing email, cyberstalking, various explicit content, vandalism, unauthorized tampering with computer systems, using misleading domain names, using another person's identity and/or identity fraud.
- **Libel Laws:** Publicly defaming people through publishing material on the Internet, email, etc.

- **Copyright Violations:** Copying, selling, or distributing copyrighted material without the express written permission of the author or publisher (users should assume that all materials available on the Internet are protected by copyright); engaging in plagiarism (using other's words or ideas as your own).

Acceptable Use Contract

Student Agreement

I understand and will abide by the provisions and conditions outlined in the Adelanto Elementary School District's Acceptable Use Policy. I understand that any violations of the Acceptable Use Policy or related District policies may result in disciplinary action, account revocation, and possible legal action and/or prosecution. I also agree to report any misuse of District technology immediately. I understand that all rules of conduct described in District and school site policies, procedures, and handbooks apply while I am using District technology resources.

Student Printed Name _____

Student ID _____

Student Signature _____

Date _____

Parent/Guardian Agreement

Students under 18 years of age must obtain the signature of a parent or legal guardian who has read this contract. As this student's parent or legal guardian, I have read this Acceptable Use Policy and understand that it is designed for educational purposes. I understand that Adelanto Elementary School District can't restrict access to all controversial materials, and I will not hold the District responsible for materials acquired on the District network. I also agree to report any misuse of District technology to the school or District staff.

I hereby give my permission to allow my child access to the technology resources provided by Adelanto Elementary School District, including the Internet.

Parent Printed Name

_____

Parent Signature **Date**

_____ _____

Parents, for further information on educating minors about appropriate online behavior, we recommend visiting http://www.onguardonline.gov. This resource is provided by the federal government free of charge. For copies of this Acceptable Use Contract, please go to http://www.aesd.net/aup.