

# Policy

## Policy and related documents

- [Do's and Don'ts for Staff](#)
- [Staff Acceptable Use Policy](#)
- [Student Acceptable Use Policy](#)
- [Do's and Don'ts for Students](#)

# Do's and Don'ts for Staff

## Do's and Don'ts

### Use of School District Computer/Laptop

**Don't** eat or drink over the keyboard and mouse or blow smoke over your screens.

**Don't** let anyone else use a district computer. It is for your use only; not your spouse, child, friend, neighbor.

**Do** password protect the computer and data.

**Don't** store students' personal information on the computer.

All district computers are protected by district licensed anti-virus software. Don't disable, remove, or add your own anti-virus software.

**Do** use a wheeled briefcase or laptop carrier to organize, move and store your laptop.

**Don't** store personal information on your computer.

**Do** store the computer properly to keep it protected and clean.

**Don't** leave the computer in the car, especially in plain sight, or in hot weather.

**Don't** clean computer with household cleaning products.

**Do** back up your data on a CD, DVD, or Flash Drive.

**Don't** view obscene, offensive, or illegal material.

**Don't** install software without permission.

**Don't** put your computer on the floor. Computers are incredibly expensive vacuum cleaners. The fans that pull air through the case to cool that hot new processor, video card and hard drive are also pulling all the

stuff that settles out of the air, and onto the floor, into your computer.

**Don't** let your pet sleep, lay or play next to your computer. This is another reason to keep your computer off the floor and on your desktop.

[Printable Copy](#)

# Staff Acceptable Use Policy

## Staff Acceptable Use Policy

## Printable PDF

### Introduction

Adelanto Elementary School District ("District") recognizes that access to technology at school gives students greater 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 21<sup>st</sup>-century technology and communication skills. To facilitate this we provide access to various technologies for student and staff use.

This Acceptable Use Policy ("Policy") outlines the guidelines and behaviors that all users are expected to follow when using District technology resources.

- The Adelanto School District network is intended solely for educational purposes.
- All activity over the network or using District resources may be monitored and retained.
- Access to online content via the network will be restricted in accordance with our policies and applicable federal regulations, such as the Children's Internet Protection Act ("CIPA").
- Users are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of technology resources may result in disciplinary action.
- Adelanto School District makes a reasonable effort to ensure our users' safety and security online but will not be held accountable for any harm or damages that result from the use of District technologies.
- Users of the District network or other technologies are expected to alert Technology Department staff immediately of any concerns for safety or security.

### Technologies Covered

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

# Usage Policies

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 Acceptable Use Contract, each user acknowledges and agrees to abide by the terms of the Policy. 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.

District technology resources are to be used for District-related business, instruction, learning, and administrative activities. Use of District technology resources to engage in personal communications is not permitted, except in an emergency.

# Internet Access

The District provides its users with access to the Internet, including web sites, resources, content, and online tools. This access will be restricted in compliance with CIPA regulations and District policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users shall comply with the access and security procedures and systems established to ensure the security, integrity and operational functionality of District computer resources.

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.

# E-mail

The District may provide users with e-mail accounts for the purpose of school-related communication. Availability and use may be restricted based on District policies.

If users are provided with e-mail accounts they should be used with care. E-mail is not a secure transmission protocol; messages are sent in clear text and may be intercepted. Users should never send personal information or attempt to open files or follow links from unknown or untrusted origin. Users shall refrain from profanity and vulgarity. Only communicate with other people as allowed by District policies or the teacher.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. E-mail usage may be monitored and archived.

# Accounts

Accounts issued to users for the use of District technology resources are for the intended user's sole use only. Users are expected to keep login information private at all times and are responsible for any misuse that occurs under the accounts issued to them. They shall use the system only under their own accounts and shall maintain the privacy of personal information and passwords.

# Social/Web 2.0 / Collaborative Content

Recognizing the benefits collaboration brings to education, the District may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should never share personally identifying information online.

# Mobile Devices Policy

The District may provide users with mobile computers or other devices to promote learning outside of the classroom. Users are expected to abide by the same acceptable use policies when using devices off the District network as on the District network. Use of these devices while off the District network may be monitored.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the District is entrusting to your care. Users should report any loss, damage, or

malfunction to Technology Department staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse.

# Personal Equipment Policy

The District recognizes that the use of certain technology devices, such as memory sticks, which are not owned by the District may be beneficial to both District employees and students.

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 and students may not connect laptops, PDAs, internet tablets, or other personal computing or mobile communication devices which are not owned or leased by the District to the District data network and/or internet service, absent express permission by the system administrator.

District employees may only use personal communication devices during non-duty 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.

## Security

Security on any computer system is of the highest priority. Users who identify a security problem must immediately notify a representative from the Technology Department or an administrator.

Users must never use another user's account and should never share passwords with anyone or leave it where it may be discovered. Under no circumstances may students be allowed to use teacher or staff computers. Any user identified as a security risk may be denied access to the system.

## Downloads

Users shall not download or attempt to download or run executable programs over the District network or onto District resources without express permission from Technology Department staff.

You may be able to download other file types, such as images or videos. To ensure the security of the network download such files only from reputable sites, and only for educational purposes. Transmission, receiving, or downloading of any material in violation of any U.S. or State regulations is prohibited. This includes, but is not limited to, copyrighted material, pornography, threatening or obscene material or images inappropriate to an instructional environment.

# Political Activities

Users shall not use District technology resources for political purposes including, but not limited to, urging the support or defeat of any ballot measure or candidate, including, but not limited to, any candidate for election to the governing board of the district.

# Netiquette

Users are expected to always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users are expected to recognize that among the vast array of valuable content online there also exists unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.

Users should also remember not to post anything online that they wouldn't want parents, teachers, future colleges or potential employers to see. Once something is online, it is out there—and can sometimes be shared and spread in ways you never envisioned or intended.

# Plagiarism

Users shall not plagiarize (or use as their own, without citing the original creator) content,

including words or images, from the Internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet must be appropriately cited, giving credit to the original author.

# Personal Safety

Users should never share personal information including phone numbers, addresses, social security numbers, birthdates, or financial information over the Internet or via e-mail.

Communicating over the Internet brings anonymity and associated risks and users should always carefully safeguard the personal information of themselves and others. Students should never agree to meet someone they have communicated with online in real life without parental permission.

If you see a message, comment, image, video or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

# No Expectation of Privacy

District technology resources and all user accounts are the property of District. There is no right to privacy in the use of the technology resources or user accounts.

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 e-mail, which is transmitted through District technology 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 technology resources.

District reserves the right to monitor and access information contained on its computer resources under various circumstances including, but not limited to, the following circumstances:

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.

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.

The contents of electronic messages, including any e-mail communication sent using District technological resources, may be viewed by a system administrator in the course of routine maintenance, or by the system administrator, or designee(s) as needed for District administrative purposes, including but not limited to, investigation of possible violations of the Policy or other District policies, and monitoring of on-line activities of minor students. Electronic mail systems store messages in files. These files are copied to back-up tapes 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.

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.

# Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber-stalking are all examples of cyberbullying. Don't send e-mails, text messages, or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to cause harm (physically or emotionally) to another person will result in severe disciplinary action and loss of privileges. Cyberbullying can be a crime. Remember that your activities are monitored and retained.

# Examples of Acceptable Use

I will:

- Use District technologies for instructional activities.
  - Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
  - Treat District resources and equipment carefully, and alert staff if there is any problem with their operation.
  - Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
  - Alert a staff member if I see threatening, inappropriate, or harmful content (images, messages, posts or videos) online.
  - Use District technologies at appropriate times, in approved places, and only for educational pursuits.
  - Cite sources when using online sites and resources for research.
- 
- Recognize that the use of District technologies is a privilege and treat it as such.
  - Be cautious to protect the safety of others and myself.
  - Help to protect the security of District resources.

# Examples of Unacceptable Use

I will not:

- Use District technologies in a way that could be harmful.
- Attempt to find inappropriate images or content, or attempt to circumvent the District's filtering tools.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- Use District technologies to send mass mailings, "spam," or "mail bombs." Mass mailings directed to "All District Employees" or to any large subgroup of District employees shall be approved by the sender's immediate supervisor.
- Plagiarize content I find online.
- Share personally identifying information, about others or myself.
- Use District technologies for personal gain, product advertisement, political lobbying, or partisan political activities.
- Use language online that would be unacceptable in the classroom.
- Use District technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, or content that is not intended for my use.

This is not intended to be an exhaustive list. Users should use their own good judgment when using District technologies.

## Limitation of Liability

The District will not be responsible for damage or harm to persons, files, data, or hardware. While the District employs, and makes reasonable efforts to ensure the proper functioning of filtering and other safety and security mechanisms, it makes no guarantees as to their effectiveness.

The District will not be responsible, financially or otherwise, for unauthorized transactions conducted over the District network.

# Violations of this Acceptable Use Policy

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 the Assistant Superintendent, Human Resources for review. The Director of ITS and/or the Assistant Superintendent, Human Resources shall then determine whether a violation of the Agreement has occurred. If the Assistant Superintendent, Human Resources 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.

# Student Acceptable Use Policy

## Student Acceptable Use Policy

## Printable PDF

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 21<sup>st</sup>-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).

# Do's and Don'ts for Students

## Do's and Don'ts

### Use of School District Chromebook

Don't eat or drink over the keyboard and mouse or blow smoke over your screen

Don't let anyone else use a district Chromebook. It is for your use only; not your sibling, friend, neighbor.

Don't disable, remove, or add your own anti-virus software. All district computers are protected by district licensed anti-virus software.

Don't store personal information on your Chromebook

Do store the Chromebook properly to keep it protected and clean

Don't leave the Chromebook in the car, especially in plain sight, or in hot weather.

Don't clean Chromebook with household cleaning products.

Don't view obscene, offensive, or illegal material

Don't install software without permission

Don't put your computer on the floor. This will clog the fans to cool the Chromebook

Don't let your pet sleep, lay or play next to your Chromebook This is another reason to keep your

Chromebook off the floor and on your desktop.

07/2023 LM

Download PDF version here: [Do's and Don'ts Students.pdf](#)