ASPEN SCHOOL DISTRICT

ACCEPTABLE USE POLICY
Policy JS-R

1. Introduction and Purpose

This Acceptable Use Policy (AUP) outlines the expectations for the responsible, ethical, and legal use of Aspen School District's technology resources by all users (students, staff, and authorized guests). Our goal is to ensure technology enhances learning, maintains safety, and complies with all laws, including the Children's Internet Protection Act (CIPA). This policy applies to all district technology and its use, on or off district property.

2. Your Responsibilities for Technology Use

As a user of Aspen School District's technology, you are expected to use good judgment and act ethically.

- **For Education and Work:** District technology is used for educational and school-related professional purposes. Limited personal use is allowed if it doesn't interfere with learning, consume excessive resources, or violate this policy.
- **Be Respectful and Ethical:** Treat others with courtesy online. Harassment, bullying, hate speech, or derogatory comments are not allowed.
- **Protect Privacy:** Do not access, share, or publish private information about yourself or others without permission. This includes personal contact information. Do not arrange face-to-face meetings with people met online without supervision. Handle sensitive district data, including student records, confidentially (per FERPA).
- **Respect Intellectual Property:** Do not plagiarize, illegally download, or share copyrighted materials. If you use AI, cite it properly as instructed by your teachers.
- **Care for Devices:** Take good care of any district-issued devices. Report any damage, loss, or malfunction immediately to school administration or IT. Prompt reporting often helps with warranty claims; however, intentional damage will likely void warranties and could result in fees and charges.
- **Keep Accounts Secure:** Your account and password are your responsibility. Do not share them. Use strong passwords and log off devices when unattended.
- **Communicate Responsibly:** Use electronic communication (email, social media, chat features) responsibly and only for educational or professional purposes. Cyberbullying, harassment, or threats are strictly prohibited.
- **Back Up Your Data:** Save and back up your personal and academic work regularly to approved storage (Google Drive). The district is not responsible for lost data due to hardware failure or accidental deletion.
- **Report Concerns:** Immediately report any violations of this AUP, suspicious online activity, or concerns about AI ethics to a teacher, administrator, or IT staff.

3. Artificial Intelligence (AI) Tools Policy

The district supports the responsible and ethical use of AI to enhance learning.

- **Approved AI Tools:** Specific AI tools that have been vetted by the IT team are permitted

on district networks and devices. This list will change as AI evolves and integrates into other educational apps; teachers and parents will be notified of district endorsed AI tools as well as updates.

- **Caution with Other AI Tools:** Using other AI tools on the district network, for assessing student work, or for student use should be approached with caution. The district prioritizes the safety and appropriateness of endorsed AI tools for teachers and students.
- **Ethical Use & Academic Integrity:** Use AI for educational purposes only, avoiding malicious or harmful activities. Students must properly cite AI use in their work as directed by teachers.
- **Evaluate Critically:** Always remember that AI-generated content can be inaccurate, biased, or incomplete. Always critically evaluate information from AI tools.
- **Protect Data with AI:** Never input confidential, personally identifiable, or sensitive district or student information into any AI tool unless explicitly authorized. Do not use AI in ways that could compromise network security or tamper with AI-generated content.

4. Prohibited Uses

The following actions are strictly forbidden when using Aspen School District's technology:

- **Illegal Activities:** Any use that violates federal, state (Colorado), or local laws, including:
  - Accessing, creating, or sharing obscene, child pornography, or harmful content.
  - Hacking or unauthorized access to systems/data.
  - Cyberbullying, threats, defamation, or libel.
  - Violating copyright or intellectual property laws.
- **Security Breaches:** Attempting to bypass security measures (firewalls, filters, VPNs), unauthorized access to accounts/files, introducing viruses or malware, launching cyberattacks, or sharing credentials. These actions are considered severe violations and will result in serious disciplinary action and may lead to legal prosecution.
- **Disrupting Services & Vandalism:** Activities that disrupt network services, waste resources, or damage district hardware/software (e.g., excessive bandwidth use, introducing viruses, unapproved encryption software).
- **Inappropriate Content:** Accessing, creating, or sharing content that is sexually explicit, threatening, discriminatory, promotes violence, or is inconsistent with the district's educational mission.
- **Unauthorized Software:** Using, downloading, or possessing any software, apps, or content not approved or properly licensed by the district, including unapproved AI tools.
- **Commercial/Political Use:** Using district technology for personal commercial activities, political lobbying, or non-school fundraising without explicit authorization.
- **Deception:** Hiding your identity or impersonating others online.

5. Access Restrictions and Personal Devices

- **Content Filtering:** The district uses filtering tools to filter inappropriate content and ensure CIPA compliance. Bypassing these filters is prohibited.
- **District Devices Preferred:** Students are provided 1:1 Chromebooks, and teachers receive district-issued devices. These are the primary devices for use on school property.
- **Personal Devices:** Any requests to use personal devices on the school network must be directed to building Principals (for students) or the IT team (for teachers). Personal devices used on the network must comply with this AUP.

6. Privacy, Monitoring, and Enforcement

- **No Expectation of Privacy:** There is no expectation of privacy when using district technology. All data and activity on district systems (internet, email, files) may be monitored, accessed, and reviewed by authorized personnel without prior notice. This monitoring is done to ensure policy compliance, manage resources, and protect users, including the use of **Blocksi**.

- **Consequences of Violation:** Violating this AUP can lead to:

  - Loss of technology privileges.
  - Disciplinary action (detention, suspension, expulsion for students; reprimand, suspension, termination for staff).
  - Legal action and/or referral to law enforcement for illegal activities.
  - Parental notification.

7. Disclaimer, Review, and Consent

- **Disclaimer:** The Aspen School District provides technology "as-is" and is not responsible for damages or lost data from its use. Use of online information is at your own risk.
- **Review and Revision:** This AUP will be reviewed annually and may be updated. Users will be notified of changes.
- **Accessibility:** The district is committed to accessible technology for all users, including those with disabilities, and will provide reasonable accommodations.
- **Consent:** By using Aspen School District's technology, you acknowledge, understand, and agree to abide by this policy.

Adopted by Administration: August 1, 2025

LEGAL REFS.: Every Student Succeeds Act (ESSA) of 2015
47 U.S.C. 254 (h) (Children's Internet Protection Act of 2000, as amended by the Broadband Data Improvement Act of 2008)
47 C.F.R. Part 54, Subpart F (Universal Support for Schools and Libraries)
C.R.S. 22-87-101 et seq. (Colorado Children's Internet Protection Act, as amended)
Colorado Privacy Act, C.R.S. 6-1-1301 et seq. (and related amendments, e.g., SB24-041)
Family Educational Rights and Privacy Act (FERPA)

CROSS REFS.: AC, Nondiscrimination/Equal Opportunity
EGAEA, Electronic Communication
JB, Equal Educational Opportunities
JICJ, Student Use of Electronic Communication Devices