



Title: **Student Use of the Internet, Electronic Communications, and Digital Media**

Code: JS

Section: Section J: Students

The utilization of the Internet, electronic communications, artificial intelligence, and digital media is integral to supporting educational curricula and substantially enriching the learning environment. Engagement with these resources necessitates students to exercise critical thinking, information analysis, effective communication, proficient writing skills, problem-solving abilities, and the cultivation of digital competencies essential for current employment demands. Moreover, leveraging these tools fosters a mindset of continual learning and provides avenues for remote education participation, peer interaction, and access to educational informational resources. For this policy's purposes, "digital resources" means District network and any device, hardware, software, website, database, or other technology used to access the Internet.

Blocking or filtering obscene, pornographic, or harmful content

Recognizing the dynamic nature of the digital landscape, wherein students may encounter materials of varying content, including potentially harmful content, the District will make reasonable measures to safeguard students from accessing material deemed obscene, pornographic, or otherwise detrimental to minors, in accordance with the Children's Internet Protection Act (CIPA). Students shall take responsibility and use good judgment when using District digital resources to avoid exposure to inappropriate material.

No expectation of privacy

District-owned digital resources are intended for educational purposes and are subject to monitoring and oversight by the District. Students should be aware that there is no expectation of privacy when accessing or using District digital resources or within the District network. Students' District-provided devices will be filtered at all times. Student personal devices are filtered while on the District network.

Unauthorized and unacceptable uses

Students shall use District technology devices in a responsible, efficient, ethical and legal manner. Unauthorized and unacceptable uses of digital resources encompass a spectrum of behaviors, including but not limited to accessing, creating, or transmitting material unrelated to educational objectives. All material and information accessed/received through the District network shall remain the property of Academy District 20 and subject to disclosure under the Colorado Open Records Act (CORA).

Because technology and ways of using technology are constantly evolving, every unacceptable use of District technology devices cannot be specifically described in policy. Therefore, examples of unacceptable uses include, but are not limited to, the following:

No student shall access, create, transmit, retransmit, generate using an Artificial Intelligence (AI) tool, or forward material or information:

- that promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons
- that is not related to District education objectives
- that contains pornographic, obscene or other sexually oriented materials, either as pictures or writings, that are intended to stimulate erotic feelings or appeal to prurient interests in nudity, sex or excretion
- that harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons in violation of the District's nondiscrimination policies
- for personal profit, financial gain, advertising, commercial transaction or political purposes
- that plagiarizes the work of another
- that uses inappropriate or profane language likely to be offensive to others in the school community
- that is knowingly false or could be construed as intending to purposely damage another person's reputation
- in violation of any federal or state law or District policy, including but not limited to copyrighted material and material protected by trade secret
- that contains information protected by confidentiality laws
- using another individual's Internet or electronic communications account
- that impersonates another or transmits through an anonymous remailer
- that accesses fee services without specific permission from the system administrator
- as a means for cyberbullying (policy JICDE)

Security and safety

Ensuring the security and safety of digital resources is of paramount importance. Students must promptly report any security concerns they encounter while using digital resources to designated District personnel. Additionally, students are prohibited from engaging in activities that compromise the integrity or functionality of District networks or digital resources, including acts of vandalism, hacking attempts or unauthorized access attempts which includes using another person's password or any other identifier. Inappropriate use or vandalism against District networks or digital resources are subject to disciplinary measures, including loss of the digital resource, loss of network privileges, suspension, expulsion, or civil or criminal liability under applicable laws.

In the interest of student safety and security, schools integrate digital citizenship and media literacy skills into instruction as part of their accreditation process. Students are reminded to exercise caution if sharing personally identifiable information (PII) and to refrain from arranging in-person meetings with individuals encountered online.

District Provided Devices (DPD)

Students must handle and maintain District-provided devices carefully to avoid fines for damages. They are responsible for the safekeeping, proper use, and accountability of these devices, including refraining from putting stickers or other modifications on the device. Damage or loss of devices must be reported to the District Technology Technician within 24 hours, and if a student leaves the District, the device must be returned at the time of disenrollment. Student DPDs must not be taken out of the country without prior authorization.

Student use is a privilege

The District emphasizes that the use of digital resources, including access to the Internet, electronic communications, artificial intelligence (AI), and digital media services, is a privilege contingent upon responsible and ethical conduct. Failure to adhere to established usage guidelines may result in the loss of access privileges, restitution for damages incurred, and disciplinary action in accordance with District policy.

School district makes no warranties

Students and parents/guardians are required to annually review the District's Student Use of the Internet, Electronic Communications, and Digital Media (JS E 1) before accessing Internet, electronic communications, or digital media accounts. It is important to note that the District assumes no liability for the content accessed or the quality of information received via digital resources, and students utilize such resources at their own risk.

Adopted/Approved: February 6, 1997

Reviewed: August 2, 2001

Revised: June 5, 1997

October 23, 2006

June 1, 2012

February 21, 2014

January 26, 2015

July 1, 2015

July 1, 2018

July 1, 2021

July 1, 2022

July 1, 2024

July 1, 2025

Legal Refs:

20 U.S.C. 6751 et seq. (Enhancing Education Through Technology Act of 2001)

47 U.S.C. 254(h) (Children’s Internet Protection Act of 2000)

47 C.F.R. Part 54, Subpart F (Universal Service Support for Schools and Libraries)

C.R.S. 22-87-101 et seq. (Children's Internet Protection Act)

C.R.S. 22-16-101 et seq. (Student Data Transparency and Security Act)

Cross Refs:

EL-2.0, Global Executive Constraint

EL-2.1, Treatment of Students

BSR-3.3, Delegation to the Superintendent

AC, Nondiscrimination/Equal Opportunity

EGAEA, Electronic Communication

JB, Equal Educational Opportunities

JICDE, Bullying Prevention and Education

JKD/JKE, Student Suspension/Expulsion/Denial of Admission

Adopted: **February 06, 1997**

Last Revised: **July 01, 2025**
