



Monument Academy

Board of Directors Governance and Policy

Policy Area: Governance	Policy #: 1517
Title: Internet Use Policy	Adopted: August 15, 2005
	Revised: October 11, 2012
	Revised: March 8, 2018
	Revised: March 11, 2021

I. Issue Statement

- A. Monument Academy is pleased to offer students and staff access to school devices, communications systems, the Internet, and other technology resources to promote educational excellence. The Board is committed to connecting teachers, administrators, and support staff with each other and with resources around the world for improved collaboration and fast access to current information.
- B. Similarly, the Board is committed to providing access to information and expert resources for all students. Students not only need access to valuable information and to available experts around the world, they also need to develop the abilities to access, locate, evaluate and apply current information. Development of these abilities is a fundamental educational objective for the 21st century.
- C. The Board's purpose is to establish a policy for use of the Internet and related resources. This policy shall apply to ALL employees, students, volunteers, or organizations with whom Monument Academy has a relationship who may have access to Monument Academy electronic assets (i.e., computers, e-mail, web sites, cell phones, network, etc.).

II. Policy Statement

- A. Access to and use of the Internet at Monument Academy is provided for the purpose of fostering communication with the academic community at-large and will be limited to direct business and academic uses only.

III. Content Filtering

- A. Internet and email use by any authorized individual is subject to monitoring, without their knowledge, and infractions of this policy may result in disciplinary action and/or denial of access. Disciplinary action may include termination of employment, suspension, or other remedies as may be available by law.
- B. To protect students from material and information that is obscene, child pornography or otherwise harmful to minors, as defined by statute, all Internet traffic is monitored and filtered in accordance with the Children's Internet Protection Act (CIPA) and C.R.S. 24-90-601. Blocking or filtering of content may be disabled by Administration, as necessary, for purposes of bona fide research or other educational projects being conducted by staff members. All requests must go through the Chief Operating Officer.

- C. It should be noted that content blocking is effective only for devices owned by Monument Academy and/or logged into Monument Academy's Wi-Fi. Monument Academy cannot monitor or control uses via 4G/5G cellular.

IV. Privacy

- A. Monument Academy devices and communications systems are owned by the school and are only intended for educational purposes and school business. Staff members and students shall have no expectation of privacy when using the Internet or communication systems.
- B. All digital storage is school property, and as such, network administrators will review files and communications to maintain system integrity and ensure that technology is used responsibly. Staff members and students should not expect that files stored on school servers and in the cloud will be kept private. Electronic communication systems are subject to the Public Records law which means that any e-mail or files sent, received, or stored on the school's technology systems could become public information (i.e., appear in a newspaper) or be subpoenaed for court purposes.
- C. Monument Academy reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of school devices, including all Internet and electronic communications access and transmission/receipt of materials and information. All material and information accessed/received through school devices shall remain the property of Monument Academy.

V. Accountability and Compliance

- A. The following behaviors are examples of actions or activities that may result in disciplinary action or other remedies available by law. The following is a listing of currently known behaviors, and is not intended to be the complete or exhaustive list of possible infractions:
1. Unauthorized attempt to break into any computer asset whether of Monument Academy or another organization.
 2. Attempting to bring down any network to which Monument Academy is connected.
 3. Visiting or "Surfing" inappropriate Web sites including, but not limited to:
 - Pornographic Materials (Photographs, Movies, Audio, Text, etc.)
 - Illegal materials (e.g., hacking instructions)
 - Multi-player game sites
 - Sites containing messages advocating hatred toward others
 4. Using Monument Academy's time and resources for personal gain.
 5. Sending threatening messages or responding aggressively to threatening messages.
 6. Sending messages that may be considered ethnic, racial, or sexual harassment.
 7. Theft or copying electronic files without permission.
 8. Sending or posting Monument Academy's confidential materials outside of Monument Academy control.
 9. Revealing security related materials (i.e., passwords, technologies, etc.) to unauthorized sources.
 10. Revealing security weaknesses and gaps in Monument Academy's systems or networks to unauthorized sources.
 11. Revealing identifying information (i.e., telephone number, home or school addresses, name, age, etc.) to unauthorized sources.
 12. Joining or acting in concert with groups whose avowed purpose is the disruption or compromise of system, networks, and related enterprises.
 13. Refusing to cooperate with a reasonable security investigation.
 14. Sending chain letters through Monument Academy sponsored or controlled electronic means (i.e., email, etc.).

VI. Related Documents

- A. 47 U.S.C. 254(h) (*Children's Internet Protection Act of 2000*)
- B. 47 U.S.C. 231 (*Child Online Protection Act of 1998*)
- C. 20 U.S.C. 6801 *et seq.* (*Elementary and Secondary Education Act*)
- D. C.R.S. 24-72-204.5 (*monitoring electronic communications*)
- E. C.R.S. 24-90-601 (*Internet Protection in Public Libraries*)
- F. C.R.S. 22-16-101 (*Student Data Transparency and Security*)
- G. Monument Academy Technology User Agreement

VII. Points of Contact

- A. The following position shall serve as points of contact for the enforcement of this policy:
President of the Board of Directors and the Chief Operating Officer