POLICY ON COMPUTERS, NETWORK & E-MAIL USE AND ELECTRONIC DEVICES

The Children's Internet Protection Act (CIPA), 47 U.S.C. §254(h)(5), and South Dakota Consolidated Statutes Section 22-24-55 require public schools to implement certain measures and actions to ensure that students are restricted from accessing inappropriate materials online using school-owned computers. The District's Acceptable Network and Internet Use Policy (hereinafter "AUP") is intended to set forth specific obligations and responsibilities of all users, including students and staff, who access the District's Network, and to ensure such use complies with the CIPA requirements. This AUP applies even when District provided equipment (laptops, tablets, iPads, etc) is used on or off premises.

ACCEPTABLE USE: The Network may be used only as a tool to support and advance the functions of the District as well as its curriculum and educational programs. Access to the District's Network is privilege not a right. Users of the Network are responsible for their behavior and communications over the Network and access to Network services will be provided only to those staff and students who agree to act in a considerate and responsible manner and in accordance with the District's AUP.

Students may use the Network only in support of educational activities consistent with the educational objectives of the Districts. Faculty and staff may use the Network primarily in support of education and research consistent with educational objectives of the District. Faculty and staff may access the Network for limited personal use but not for any commercial or business use; however, such personal use may not violate any applicable rules and regulations or interfere with job performance. Use of the Network must be in compliance with applicable laws, including all copyright laws and all materials on the Networks should be presumed to be copyrighted. Students and staff will only be allowed access to the school internet via their district issued device, no personal devices will be granted network access.

All members of the staff who wish to use the Network must sign this AUP whenever requested by the district, to confirm that the staff person has read and understands this policy and agrees to abide by it. Each student must sign this AUP annually to confirm that the student has read and understands this policy and agrees to abide by it. Students who are under 18 must have their parents or guardians sign this AUP and submit it to the District.

INTERNET SAFETY: It is the policy of the District to protect computer users from harassment and unwanted or unsolicited electronic communications. The District cannot guarantee that users will not encounter inappropriate or offensive material on the Internet. If offensive material would cause the user embarrassment or other damage, the user should not use the system or report it to a teacher or administrator. The Montrose School District will make every reasonable effort to provide access to educationally appropriate resources, including Internet sites. However, it may not be technologically possible to limit Internet access to only those educationally appropriate sites that have been designated for the purpose of instruction, and research related to the curriculum.

It shall be the responsibility of all personnel of this district to monitor students' online activities and use of the network to ensure that their uses is in compliance with CIPA and this policy. The state issued FortiAnalyzer program will be used to look at students and staffs internet history if needed.

NETWORK ETTIQUITTE: Users are expected to abide by generally accepted rules of network etiquette. These include but are not limited to:

a) Be polite and don't become abusive to others. Do not send or encourage others to send messages that are abusive or harassing.
b) Use appropriate language. Swearing and use of vulgarities will not be tolerated.

INAPPROPRIATE USE PROHIBITED

Inappropriate use includes, but is not limited to: intentional uses that violate the law, that are specifically named as violations in this policy, that violate the regulations of the school district or any other use that hampers the integrity or security of the school district's computer network or any computer networks

connected to the Internet. The district reserves the right to define prohibited use of the Network, adopt rules and regulations applicable to Network Use, determine whether an activity constitutes a prohibited use of the Network, and determine the consequences of such inappropriate use. Prohibited use includes but is not limited to the following:

a) Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
b) Criminal activities that can be punished under law
c) Illegal installation or transmission of copyrighted material
d) The unauthorized collection of email addresses ("harvesting") of e-mail addresses for the Global Address List and other Districts directories
e) Obtaining and/or using anonymous email sites: spamming, spreading viruses
f) Bypassing of the District's filter to access blocked sites or use of anonymous proxy servers to negate firewall/filtering system
g) Disclosure of minors personal information without proper authorization
h) Causing harm to others or damage to their property, such as:
a. Deleting, copying, modifying, or forging other users names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous emails
b. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance
c. Using any District device to pursue "hacking" internal or external to the District, or attempting to access information protected by privacy laws
d. Accessing, transmitting, or downloading larges files, including "chain letters" of any type of "pyramid schemes"
i) Engaging in uses that jeopardize access or lead to unauthorized access to others' accounts or other computer networks, such as:
j) Using another's account password(s) or identifiers(s)
k) interfering with other's ability to access their account(s)
l) Disclosing your own or anyone's password to others or allowing them to use your or another's account
m) Using the network or Internet for Commercial purposes

OFF-SITE USE OF NETWORK

Students under the age of 18 should only access District-assigned email accounts and/or other Network components including but not limited to school-assigned computers laptops, tablet, or iPads off-site if a parent or legal guardian supervises their usage at all times. The students' parent or guardian is responsible for monitoring the minors off-site use of the Network and ensuring use complies with this AUP. Off-site filter will be in place on all devices leaving the district.

VIOLATIONS AND CONSEQUENCES

Violations of school district policy or the law through the use of the school district's e-mail and Internet access may result in disciplinary action. Disciplinary action may be suspension or revocation of email and/or internet privileges, detention, in-school suspension, out-of school suspension, or expulsion. Students shall be afforded due process consistent with school district policy and state law. Suspected violations of law shall be reported to the proper authorities.

The Montrose School District will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, blogging, and cyber-bullying awareness response. The superintendent is delegated authority to implement these educational requirements.

Adopted: January 13, 1997
Amended: April 14, 2008
Amended June 11, 2012
Amended March 11,2019