MVISD Parent Acceptable Use and Internet Safety Policy

The Superintendent and the technology coordinator will oversee the District's technology resources, including electronic communications systems and electronic equipment.

The District makes technology resources available to staff, students, parents, and members of the public as applicable and in accordance with the District's conditions of use. Available technology resources may include onsite internet access, District-owned hardware and software, District-approved online educational applications for use at school and at home, and digital instructional materials.

The Superintendent will designate the Director of Technology to oversee development and implementation of an internet safety plan, including guidelines for the acceptable use of the District's technology resources in compliance with this plan. All users will be provided copies of acceptable-use guidelines and training in proper use of the District's technology resources that emphasizes ethical and safe use.

The Superintendent will appoint a committee, to be chaired by the technology coordinator, to determine appropriate use of filtering devices. The Superintendent will designate the Director of Technology to oversee internet safety plans to implement and maintain appropriate technology for filtering material considered inappropriate or harmful to minors. All internet access will be filtered for minors and adults on the District's network and computers with internet access provided by the school.

The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to, nudity or pornography; images or descriptions of sexual acts, illegal use of weapons or drugs, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and online gambling. Policy allows a filter to be disabled for approved purposes only.

Access to the District's technology resources will be governed as follows:

Students:

1. Students in kindergarten–grade 5 will be granted access to the District's technology resources as determined by the campus principal.

2. Elementary students will have access to District-managed online educational applications and will not be issued or asked to create individual accounts using personally identifiable information.

3. Elementary students in grades 2nd-12th may have access to District-issued email or network accounts only as approved by the campus principal and only with parental permission. Grade 2nd-5th will only have internal domain email rights. With parental approval, students in grades

6th–12th will be assigned individual accounts and passwords for use of District sponsored technology resources, including individual email accounts and District-approved online educational resources.

4. Students granted access to the District's technology resources must complete any applicable user training, including training on cyberbullying awareness and response, copyright piracy, cybersecurity, and appropriate online behavior and interactions with other individuals on social media networking websites.

5. Parental notice and approval will be required before a student may take part in District-sponsored social media, online instructional programs, or other online or mobile educational applications, including video sharing for classroom use or use of a student's photo on a District or classroom website, even if public access is blocked.

6. Upon request from a parent, the District will provide a list of technology resources for use by the student.

Nonschool Users:

1. Nonschool users may be given limited access to District technology resources when available, including computer and internet access, online job applications, and access to the District's wireless internet, in accordance with guidelines established by the campus or the District.

2. Use of District technology resources by members of the public may not interrupt instructional activities or burden the District's network.

Student Participation in Social Media:

A student may use District technology resources to participate in social media with parental consent and only as approved by the District in accordance with the student's age, grade level, and approved instructional objectives. This includes text messaging, instant messaging, email, web logs (blogs), electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posted on the internet, and approved social networking sites.

Student Training on Safety and Security:

Students participating in social media using the District's technology resources will receive training to: Assume that all content shared, including pictures, is public; Not share personally identifiable information about themselves or others; Not respond to requests for personally identifiable information or respond to any contact from unknown individuals; Not sign up for unauthorized programs or applications using the District's technology resources; Understand the risks of disclosing personal information on websites and applications using the students'

own personal technology resources; and Use appropriate online etiquette and behavior when interacting using social media or other forms of online communication or collaboration.

Approval of Technology Resources:

The District will ensure that all technology resources in use in the District meet state, federal, and industry standards for safety and security of District data, including a student's education records and personally identifiable information. Before use in the classroom, use with students, or administrative use, any professional staff wanting to use an online learning resource, online or mobile application, digital subscription service, or other program or technology application requiring the user to accept terms of service or a user agreement, other than a District-approved resource, must first submit an application for approval. If approved, additional parental notification or permission may be required before use by students. No student 13 years of age or younger will be asked to download or sign up for any application or online account using his or her own information. For elementary students, only applications that allow for one classroom or administrator-run account will be approved.

The District has designated the following staff person as the Director of Technology:

Name: Anthony Eilers
Position: Director of Technology
Email: aeilers@mtvernonisd.net
Phone number: (903)537-9919

The Director of Technology for the District's technology resources will:

1. Assist in the development and review of responsible-use guidelines, the District's internet safety plan, the District's cybersecurity plan, and the District's security breach prevention and response plan.

2. Be responsible for disseminating, implementing, and enforcing applicable District policies and procedures, the internet safety plan, the acceptable use guidelines for the District's technology resources, and the District's breach-prevention and response plan.

3. Provide training to all users regarding safe and appropriate use of the District's technology resources, including cyberbullying awareness and response, data security, and cybersecurity measures. The technology coordinator or designee will provide training to all employees within 30 days of hire and will provide annual training to all employees.

4. Collect and maintain evidence related to incidents involving the District's technology resources, as requested by the administration.

5. Notify the appropriate administrator of incidents requiring District response and disciplinary measures, including incidents of cyberbullying.

6. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.

7. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure student safety online and proper use of the District's technology resources.

8. Coordinate with the District's records management officer to develop and implement procedures for retention and security of electronically stored records in compliance with the District's records management program.

9. Coordinate with the District webmaster to maintain District, campus, and classroom websites, consistent with the District's policies.

10. Coordinate with the District's cybersecurity coordinator about any known or suspected cybersecurity violations.