Green Mountain School
Student Acceptable Internet, Technology, Computer Use Agreement

Student use of the internet, computers, and other technology at Green Mountain School is allowed and encouraged **only** when it is part of the educational program and objectives of the school. Student access to computers and the internet varies with the age of the student. In Kindergarten through grade 2, students have limited access and are highly supervised. In grades 3-5, students are closely supervised, but begin to have independent access for research and other school purposes. In grades 6 through 8, students are given more independence to use computer resources in support of their learning. This increased computer access requires students to be responsible users of technology. Students will be issued a school-owned email account and online access to Microsoft programs to be used for school-related purposes only.

The use of internet, technology, and computer resources is a **privilege** rather than a right. Like all district resources, district internet and computer/network resources are public property, and must be used only for approved activities. The unauthorized use of these resources is a violation of school rules, district policies, and may in some cases also be a violation of the law.

In using internet and technology of the Green Mountain School District, each student must ensure that they:

- use district technology only for school-related work and approved activities
- comply with current legislation, state and federal laws, and school district policies
- use internet resources, technology, and email in an acceptable way under this agreement
- do not create any unnecessary risk to the school district by misusing the internet, email, and/or other technology or electronic services

Unacceptable Uses:

Any of the following uses of district resources by a student is unacceptable and a violation of district rules:

- use of the internet or computer without a staff member present. Students must be supervised by a staff member when using computers, technology, or when accessing the internet.
- connecting a personal computer, tablet, phone, or other device to the school wireless (WiFi) system or network without the written permission of the superintendent.
- accessing a personal email account on school equipment or through the school internet unless specific permission is given by a the superintendent; use of personal email accounts violates this agreement.
- accessing internet sites that contain obscene, hateful, pornographic, illegal gaming or otherwise illegal material (unintentional receiving of such material is not a violation if reported immediately).
- distributing, sharing or storing images, text or materials that might be considered indecent, pornographic, obscene, or illegal; distributing, disseminating or storing images, text or other materials that might be considered discriminatory, offensive or abusive, or anything that is a personal attack, threat, sexist or racist, or might be considered to be bullying or harassment of any person.
- using network resources to attempt or carry out any form of fraud, or any form of software, film, video, or music piracy; storing personal media files including photographs, music, videos, etc.
- communicating through any blog, wiki, social networking site, instant messaging, or other software or technology unless given specific permission by the superintendent; communications not directly related to classwork or the school program are a violation of this agreement.
- accessing copyrighted information in a way that intentionally violates the copyright, or using district computer or network resources to mass store or share copyrighted music or video files.
- use of school technology resources to set up or conduct for-profit business or activities for personal gain, or to carry out any business not related to the school program.
- any form of electronic trespass, including but not limited to accessing, breaching, or deleting computer systems, accounts, or files without authorization, or using District resources to hack or breach systems, accounts, or files.
- any deliberate activities that waste class time or networked resources, including the use of any social media or similar software or websites during school hours.
- purposely introducing any form of computer virus or malware into the school network.

- any attempt to hide or conceal internet activity, including the use of a proxy site or software to bypass or avoid internet filtering. Deleting or clearing internet browsing history and emails violates this rule.
- purposely changing any computer setting without permission in a way that it interferes with the use of equipment by others or which requires staff to take corrective action.
- intentionally damaging school computer equipment or misusing school computer equipment in a way that is likely to cause damage; this includes removing keys, having food or drink near computers, any form of vandalism, inserting items into ports, etc.

Internet Access/Passwords

- Student IDs and passwords help maintain individual accountability for internet usage. Students are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account.
- Under no circumstances should a student share his or her user ID or password to another student.

Filtering and Monitoring

The district maintains the right to examine any systems and inspect any data recorded in those systems in order to assure compliance with this agreement and district policy. Computer files and school email accounts are not private. District staff may access student files to verify compliance with this policy or when there is a reasonable expectation that a search of computer files will reveal a violation of school rules.

All student access to the internet will be filtered as required by the Children's Internet Protection Act (CIPA). Individuals should be aware that filtering software and network systems generate logs of the activities.

Consequences

Inappropriate/illegal use of the Green Mountain School District's internet or network resources may result in restriction of the student's privileges to use some or all forms of technology. In some cases, violations may result in further discipline up to and including suspension from school. Violations such as threats, vandalism, bullying, and harassment will be dealt with as regular discipline. Students and parents are advised that the district is required to report certain suspected violations of the law to police.

Progressive discipline guidelines:

- First Violation: Warning, possible notice to parents
- Second Violation: Loss of privileges – minimum 5 to maximum 30 days
- Third Violation: Loss of privileges – minimum 10 to maximum 60 days

Serious violations (such as pornography, trespass, or vandalism) may result in greater consequences on a first violation. The determination of consequences is at the discretion of the superintendent.

Agreement

All students are required to sign this agreement confirming their understanding and acceptance of this policy prior to being granted internet and network access and a student email account.

By signing below, the student and parent acknowledge they have read and understand this Acceptable Use Agreement, and the student agrees to not engage in any unacceptable use of the Green Mountain School District's internet, technology, or computer resources.

_____ _____

Student Name (printed) Student Signature

_____ _____

Parent Signature Date