File: JS-Rev. 2

# Internet Acceptable Use Policy for Students

All forms of electronic communication have vast potential to support curriculum and student learning while on and off school grounds. The Charter Board believes they should be used in schools as a tool to educate.

Electronic communications require students to think critically, analyze information, write clearly, use problem-solving skills, and to hone digital world skills that employers demand. Use of these tools also encourages an attitude of lifelong learning.

Technology offers a fluid environment in which students may access applications, research an unlimited amount of information, collaborate, create inform and share. While it is impossible to predict with certainty what information students may come into contact with, the charter school shall take reasonable steps to protect students from accessing material and information that is unsuitable on school grounds. This filtering will include such groups as, Malicious Intent, Adult/Sexually Explicit, Gambling, Games, Hacking, Intimate Apparel & Swimwear, Peer-to-Peer, Personals and Dating, and Proxies & Translators.

**Blocking and Filtering Process**

The charter school meets all C.D.E., C.I.P.A., and ERATE requirements for filtering and logging internet traffic provided by the charter school for students. This is for all student devices across school grounds. The charter school is not responsible and has no control over internet access that is available on school grounds by a third party.

**Security**

Security on charter school computer systems is a high priority. Students who identify a security problem while using the Internet or electronic communications must immediately notify a system administrator. Students should not demonstrate the problem to other users. Logging in as another user other than yourself is prohibited.

Students shall not:

- Use another person's password or any other identifier
- Gain or attempt to gain unauthorized access to charter school computers or computer systems
- Read, alter, delete or copy, or attempt to do so, electronic communications of other system users
- Use proxies, remote sessions, tunneling, or any other technique to bypass the charter school filtering and firewall

Any user identified as a security risk, or as having a history of problems with other computer systems, may be denied access to the Internet and electronic communications.