REGULATIONS FOR ACCEPTABLE USE OF
DISTRICT TECHNOLOGY BY STUDENTS
McHenry Community High School District 156

1. **Acceptable Use.**
   All users of the District Technology System ("System") must comply with the District Acceptable Use Regulations, as set forth below.

   The "System" shall include all computer hardware and software owned or operated by the District, the District's electronic mail, the District's web site, and the District's on-line services. "Use" of the System shall include any and all access to the System, whether by District owned computers or via remote access from any other computer terminal.

   The System, including all information and documentation contained therein, is the property of the District except as otherwise provided by law. Therefore, students have no expectation of privacy in their use of the System. The District has the right to access, review, monitor, copy, delete, or disclose, as allowed by law, any file, document, information or message sent, received, accessed or stored on the District's Technology System, including information obtained on the Internet.

2. **Privileges and Acceptable Use.**
   Access to the System is provided as a privilege by the District and may be revoked at any time. Inappropriate use may result in discipline, including, but not limited to, loss of System use privileges, suspension and expulsion.

   Technology System is part of the curriculum and is not a public forum for general use. Students may access the System only for educational purposes. The actions of students utilizing the System reflect on the School District; therefore, students must conduct themselves accordingly by exercising good judgment and complying with these Regulations and any accompanying administrative policies or regulations.

   Students are responsible for their behavior and communications using the System and will:
   a. Exhibit digital citizenship as defined by the student handbook.

   b. Use or access the network system only for educational purposes and uses deemed as appropriate in accordance with the student handbook.

   c. Use the "MCHS Student" wireless network while using their personal devices on school grounds (not personal data plans or neighboring networks) so that District #156 can abide by the student filtering guidelines of the Children's Internet Privacy Act.

   d. Comply with copyright laws and software licensing agreements.

   e. Understand that files and communications on the System are not private. Network administrators and other designated school officials may access all files and communications to maintain system integrity and monitor responsible use.

   f. Respect the privacy rights of others and maintain confidentiality of all personnel and student records.

g. Be responsible at all times for the proper use of technology, including proper use of access privileges, complying with all required system security identification codes, and not sharing any codes or passwords.

h. Maintain the integrity of the System from potentially damaging messages, physical abuse, viruses, or other vandalism.

i. Abide by the policies and regulations of networks and systems linked by technology.

j. Respect the right of others to use the System.

3. **Prohibited Use.**
The uses of the System listed below are prohibited and may result in discipline or other consequences as provided in section 8 of these Regulations and the District's Student Discipline Code and rules. The System shall **not** be used to:

a. Engage in activities which are not related to District educational purposes or which are contrary to the instructions from supervising District employees as to the System's use.

b. Access, retrieve, or view obscene, profane or indecent materials.

c. Access, retrieve, view or disseminate any material in violation of federal or state laws or regulation or District policy or rules. This includes, but is not limited to, improper use of copyrighted material; improper use of the System to commit fraud or with the intent to commit fraud; improper use of passwords or access codes; or disclosing personal information of any student, District employee, or System user.

d. Transfer any software to or from the System without authorization from the System Administrator.

e. Engage in for-profit or non-school sponsored commercial activities, including advertising or sales.

f. Harass, threaten, intimidate, bully or demean an individual or group of individuals.

g. Disrupt the educational process, including use that is reasonably foreseeable to result in a disruption, or interfere with the rights of others at any time, either during school days or after school hours.

h. Disrupt or interfere with the System.

i. Gain unauthorized access to, or vandalize, the data or files of another user.

j. Gain unauthorized access to, or vandalize, the System or the technology system of any other individual or organization.

k. Forge or improperly alter electronic mail messages, use an account owned by another user, or disclose the user's individual password or that of another user.

l. Invade the privacy of any individual, including violating federal or state laws regarding limitations on the access to, or disclosure of, student records.

m. Download, copy, print or otherwise store or possess any data which violates federal or state copyright laws or these Regulations.

n. Send nuisance electronic mail or other online messages such as chain letters, pyramid schemes, or obscene, harassing or other unwelcome messages.

o. Send mass electronic mail to multiple users without prior authorization by the appropriate District Administrator.

p. Conceal or misrepresent the user's identity while using the System.

q. Post material on the District's web site without authorization from the appropriate District Administrator.

r. Violation of any other District policy or state or federal law.

4. **Web sites.**
All subject matter on the District website or its web pages must be related to District-authorized curriculum, instruction, activities or other general information relating to the District and its mission. Unless otherwise allowed by law, District web sites shall not display student information, photographs or works of students without parental consent. Students must obtain prior approval from a teacher before publishing any web page or web content on the District's web site. Any web site or content published by a student on the District's web site must conform to these Acceptable Use Regulations.

5. **Social Media**.
Social media sites can be a useful educational tool and effective method of sharing information. Use of social media sites should be appropriate and conform to the student handbook. Use of social media to harass, threaten, intimidate, bully, or demean an individual or group of individuals is prohibited.

6. **Disclaimer.**
The District makes no warranties of any kind whether express or implied for the System. The District is not responsible for any damages incurred, including the loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions. Use of any information obtained via the System is at the user's own risk. The District is not responsible for the accuracy or quality of information obtained through the System, breaches of confidentiality, defamatory material, or for any user's intentional or unintentional access of material on the Internet which may be obscene, indecent, or of an inappropriate nature.

7. **Security and User Reporting Duties.**
Security in the System is a high priority and must be a priority for all users. Students are prohibited from sharing their login IDs or passwords with any other individual. Any attempt to log in as another user will result in discipline. A user who becomes aware of any security risk or misuse of the System must immediately notify a teacher, administrator or other staff member. Failure to do so may result in discipline.

8. **Vandalism.**
Vandalism or attempted vandalism to the System is prohibited and will result in discipline as set forth in section 8

of these Regulations, and in potential legal action. Vandalism includes, but is not limited to, downloading, uploading, or creating computer viruses.

9. **Theft of Electronic Devices.**
   Because education is moving towards increased use of personal electronic devices for educational purposes, students should be aware that theft of a district, student, or staff member owned electronic device will lead to out of school suspension and police involvement. Depending on the value of the device this could be treated as a felony by law enforcement.

10. **Unauthorized Videotaping or Photographing.**
    Unauthorized videotaping or photographing of any student or staff member with any electronic device can be considered harassment which could lead to disciplinary action ranging from suspension to expulsion. Administrators may report such incidents to local law enforcement agencies.

11. **Consequences for Violations.**
    A student who engages in any of the prohibited acts listed above shall be subject to discipline, which may include: (1) suspension or revocation of System privileges, (2) other discipline including, but not limited to, suspension or expulsion from school, and (3) referral to law enforcement authorities or other legal action in appropriate cases.