

TECHNOLOGY SYSTEM USE POLICY
McHenry Community High School District 156

It is the policy of the Board of Education of McHenry Community High School District 156 to promote the use of technology that supports learning, enhances instruction, and improves communications between the school and community.

For purposes of this policy, implementing rules, and acceptable regulations, the term “District Technology System” or “System” shall include all computer hardware and software owned or operated by the District, District electronic mail, District web sites, and District on-line services. “Use” of the District Technology System shall include use of, or obtaining access to, the System from any computer terminal whether or not owned or operated by the District.

The District Technology System is intended to support the District’s curriculum. Accordingly, the District’s Technology System is for educational use only and does not constitute a public forum. Except as provided by federal and state statutes protecting the confidentiality of students’ education records, no user of the District Technology System has an expectation of privacy in connection with such use.

The Board of Education recognizes that although the Internet and on-line services afford access to legitimate sources of information for academic and educational purposes, they also enable access to materials which may be illegal, obscene or indecent. Use of the District Technology System, including the Internet, shall be consistent with the District’s educational mission and curriculum adopted by the Board.

The Board of Education further recognizes that the effective operation of the District Technology System depends upon the existence and enforcement of regulations for the efficient, ethical and legal use of its resources. The Administration is authorized to and shall adopt and enforce regulations which limit the use of the System to educational purposes, and describe acceptable and ethical use of the System.

Such regulations shall be distributed to District employees and students of the District 156 community who are afforded access to the System.

Violation of the acceptable use regulations shall be subject to consequences including, but not limited to, discipline, loss of System use privileges, and referral to law enforcement authorities or other legal action in appropriate cases.

The Board of McHenry Community High School District 156 adopted this Technology System Use Policy at a public meeting following normal public notice, on August 5, 2008.

INTERNET SAFETY POLICY
McHenry Community High School District 156

Introduction

It is the policy of McHenry Community High School District 156 to:

- (a) Prevent access to, or the transmission of, inappropriate and/or unlawful material via Internet, electronic mail, or other forms of direct electronic communications.
- (b) Prevent unauthorized online disclosure, use, or dissemination of the personal identification information of staff or students.
- (c) Comply with the Children's Internet Protection Act [47 USC 254(h)].

Definitions

Key terms are as defined in the Children's Internet Protection Act.

Access to Inappropriate Material

In accordance with the Children's Internet Protection Act, the District installs and operates software to limit users' Internet access to materials that are obscene, pornographic, harmful to children, or otherwise inappropriate, notwithstanding that such software may in certain cases block access to other materials as well. At the same time, the District cannot guarantee that filtering software will in all instances successfully block access to materials deemed harmful, indecent, offensive, pornographic, or otherwise inappropriate. The use of filtering software does not negate or otherwise affect the obligations of users to abide by the terms of this policy and to refrain from accessing such materials.

Supervision and Monitoring

It shall be the responsibility of McHenry Community High School District 156 staff to supervise and monitor student usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act. Subject to staff permission and supervision, technology protection measures may be disabled or, in the case of students, minimized, only for bona fide research or other lawful purposes.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director of Network Technology Services or designated representatives.

Adoption

The Board of McHenry Community High School District 156 adopted this Internet Safety Policy at a public meeting, following normal public notice, on August 5, 2008.

**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. Use or access the System only for educational purposes.
- b. Comply with copyright laws and software licensing agreements.
- c. 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.
- d. Respect the privacy rights of others and maintain confidentiality of all personnel and student records.
- e. 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.

- f. Maintain the integrity of the System from potentially damaging messages, physical abuse, viruses, or other vandalism.
- g. Abide by the policies and regulations of networks and systems linked by technology.
- h. 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 written parental permission. 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. 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.

6. 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.

7. 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.

8. 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.

**AUTHORIZATION FOR ACCESS TO
DISTRICT TECHNOLOGY SYSTEM BY STUDENTS**

McHenry Community High School District 156



This form must be read and signed by each student (and if under age 18 by his/her parent/guardian) as a condition of using the District Technology System.

By signing this Authorization, I acknowledge that I have received a copy of the "Regulations for Acceptable Use of District Technology System by Students" dated August, 2008, and that I have read, understand, and agree to follow the Regulations.

I acknowledge that access to the District Technology System is provided as a privilege by the District and that inappropriate use may result in discipline, as may off-site use of electronic technology which disrupts or can reasonably be expected to disrupt the school environment.

I ACKNOWLEDGE THAT I HAVE NO EXPECTATION OF PRIVACY IN MY USE OF THE DISTRICT TECHNOLOGY SYSTEM, AND THAT THE DISTRICT HAS THE RIGHT TO AND DOES MONITOR USE OF THE SYSTEM.

Parent/Guardian permission for student to access the Internet:

YES

NO

Student Name: _____

Grade: _____

Student Signature: _____

Date: _____

Parent/Guardian Name: _____

Parent/Guardian Signature: _____

Date: _____