MSBA/MASA Reviewed: 2012 *Previous Adoption: August 12, 2012*
Reviewed by YME Tech Committee, Administrators, and Policy Committee: March 2013
First Reading: April 8, 2013
Second Reading: May 13, 2013
Adopted: May 13, 2013

524 INTERNET ACCEPTABLE USE AND SAFETY POLICY (Mandatory Policy)

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for access to the school district computer system and acceptable and safe use of the Internet, including electronic communications.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student and employee access to the school district computer system, electronic resources, and the Internet, including electronic communications, the school district considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the school district computer system, electronic resources, and to the Internet enables students and employees to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. The school district expects that faculty will blend thoughtful use of the school district computer system, electronic resources, and the Internet throughout the curriculum and will provide guidance and instruction to students in their use. This policy shall apply to all users of the School District's computer system, electronic resources, and Internet, including but not limited to students, faculty, administrators, support staff, agents and board members. This policy shall apply to the use of the School District's electronic resources provided by any means, including but not limited to: desktop computers, laptop computers, PDAs, Smart Devices, printers, mobile devices (wireless), network servers.

III. LIMITED EDUCATIONAL PURPOSE

The school district is providing students and employees with access to the school district computer system, which includes Internet access. The purpose of the system is more specific than providing students and employees with general access to the Internet. The school district system has a limited educational purpose, which includes use of the system for classroom activities, educational research, and professional or career development activities. Users are expected to use Internet access through the district system to further educational and personal goals consistent with the mission of the school district and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network. Proper use of the School District's Internet access and electronic resources is the responsibility of the individual user.

IV. USE OF SYSTEM IS A PRIVILEGE

The use of the school district system and access to use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the school district system or the Internet may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate school district policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under other applicable laws.

V. SYSTEM/PROPERTY RIGHTS

The information, communication, processing, and storage resources provided by the School District are the sole property of the District. Files, data, and other communication created originating from, or stored on the District's hardware, software, equipment and software leased from others by the School District are considered the District's property for the purposes of this policy. The District's ownership and control over its systems shall apply regardless of how and where a user accesses the District's systems.

One fundamental need for acceptable student and employee use of District electronic resources is respect for, and protection of, password/account code security, as well as restricted databases, files, and information banks. Personal passwords/account codes shall be created to protect students and employees utilizing electronic resources to conduct research or complete work.

VI. UNACCEPTABLE USES

All School District systems, equipment and electronic resources must be used for educational or educational related purposes. The following uses of the school district system and Internet resources or accounts are considered unacceptable:

A. Users will not use the school district system to access, review, upload, download, store, print, post, receive, transmit or distribute:

1. pornographic, obscene or sexually explicit material or other visual depictions that are harmful to minors;

2. obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;

3. materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;

4. information or materials that could cause damage or dager of disruption to the educational process;

5. materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.

B. Users will not use the school district system to knowingly or recklessly post transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

C. Users will not use the school district system to engage in any illegal act or violate any local, state or federate statute or law.

D. Users will not use the school district system to vandalize, damage or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means, will not tamper with, modify or change the school district system software, hardware or wiring or take any action to violate the school district's security system, and will not use the school district system in such a way as to disrupt the use of the system by other users.

E. Users will not use the school district system to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.

F. Users will not use the school district system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs or other information that would make the individual's identify easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message.

1. This paragraph does not prohibit the posting of employee contact information on school district webpages or communications between employees and other individuals when such communications are made for education-related purposes (i.e., communications with parents or other staff members related to students).

2. Employees creating or posting school-related webpages may include personal contact information about themselves on a webpage. However, employees may not post personal contact information on other personally identifiable information about students unless:

a. such information is classified by the school district as directory information, and verification is made that the school district has not received notice from a parent/guardian or eligible student that

such information is not to be designated as directory information in accordance with Policy 515; or

b. such information is not classified by the school district as directory information but written consent for release of the information to be posted has been obtained from a parent/guardian or eligible student in accordance with Policy 515.

In addition, prior to posting any personal contact or personally identifiable information on a school-related webpage, employees shall obtain written approval of the content of the postings from the building administrator.

c. These prohibitions specifically prohibit a user from utilizing the school district system to post personal information about a user or another individual on social networks, including, but not limited to, social networks such as "MySpace" and "Facebook."

G. Users must keep all account information and passwords on file with the designated school district official. Users will not attempt to gain unauthorized access to the school district system or any other system through the school district system, attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user. Messages and records on the school district system may not be encrypted without the permission of the appropriate school authorities.

H. Users will not use the school district system to violate copyright laws or usage license agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school computer, and will not plagiarize works they find on the Internet.

I. Users will not sue the school district system for conducting business, for unauthorized commercial purposes or for financial gain unrelated to the mission of the school district. Users will not use the school district system to offer or provide goods or services or for product advertisement. Users will not use the school district system to purchase goods or services for personal use without the authorization from the appropriate school district official.

J. Users will not waste electronic resources (using bandwidth), including recreational Internet surfing.

K. Users will not engage in job search activities for positions outside of the school district.

L. Users shall not use or install hardware, modems, web servers, software or other equipment on the YME system. Any equipment or software brought into YME for use in a classroom, office or lab setting may not be used unless being donated

to the YME School District or with the express prior permission of the system administrator in conjunction with the building principal.

M. A student or employee engaging in the foregoing unacceptable uses of the Internet when off school district premises also may be in violation of this policy as well as other school district policies. Examples of such violations are, but are not limited to, situations where the school district system is compromised or if a school district employee or student is negatively impacted. If the school district receives a report of an unacceptable use originating from a non-school computer or resource, the school district may investigate such reports to the best of its ability. Students or employees may be subject to disciplinary action for such conduct, including, but not limited to, suspension or cancellation of the use or access to the school district computer system and the Internet and discipline under other appropriate school district computer system and the Internet and discipline under other school district policies, including suspension, expulsion, exclusion or termination of employment.

N. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school district official. In the case of a school district employee, the immediate disclosure shall be to the employee's immediate supervisor and/or the building administrator. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. In certain rare instances, a user may also access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher or, in the case of a school district employee, the building administrator.

VII. ONLINE SAFETY

Internet safety awareness is based on an ongoing program of education within the school for all learners. This instruction includes but is not limited to: appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. In order to assist children and young people to stay safe when using technology, staff receive continual instruction and information on existing and emerging technologies. The requirement to raise awareness in children and young people of the risks associated with inappropriate contact via the Internet and content on the Internet is therefore addressed as part of the wider duty of care to which all staff are bound. It is essential that all learners are taught the relevant skills and strategies to remain safe. Therefore, online safety tools are embedded within all curriculum areas.

VIII. ACCESS RULES

A. Student email is allowed only through District controlled accounts. Written parental/guardian permission is required before an account is granted.

B. Users shall not use any Internet Access or service provider other then the access or service provider that is supplied and made available to user by the School District.

C. Users shall only use software supplied by the School District.

D. Employee users shall not install hardware or software on the School District's systems without the express prior permission of their supervisor or the District Technology Coordinator. Students may not install hardware or software unless it is for instructional purposes in the classroom setting, and have been directed to do so by the District Technology Coordinator.

E. Users shall not access, modify, or delete the files belonging to other users. Users shall use only the user names provided by the School District.

F. FTP (File Transfer Protocols)/Telnet

1. Users shall not open files received from the Internet without first conducting a virus scan of the file.

2. Users shall not transfer files using the School District's electronic resources without the approval of the District Technology Coordinator.

3. Applications used to access other computer systems are strictly prohibited except for instructional purposes. For example, Telnet applications, remote administration software, or any other related software/hardware that would allow access to another system.

G. All use of electronic resources of the School District shall be in compliance with all other School District policies.

H. Students access shall be subject to such additional rules, limitations and conditions as may be set by their instructor(s).
Employee Access shall be subject to such additional rules, limitations and conditions as may be set by their supervisor(s).

IX. SECURITY

Every user must maintain the security of the School District electronic information systems. Users shall not divulge passwords or security protocols to anyone. Users shall not permit non-employees/unauthorized users access to the School District's electronic resources.

X. FILTER

A. With respect to any of its computers with Internet access, the School District will monitor the online activities of minors and employ technology protection

measures during any use of such computers by minors and adults. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:

1. Obscene;

2. Child pornography; or

3. Harmful to minors.

B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:
   1. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or
   2. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

C. Taken as a whole. Lacks serious literary, artistic, political, or scientific value as to minors,

D. An administrator, supervisor or other person authorized by the Superintendent may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.

XI. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the school district computer system and use of the Internet shall be consistent with school district policies and the mission of the school district.

XII. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of the school district system, the school district does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal files on the school district system.

B. Routine maintenance and monitoring of the school district system may lead to a discovery that a user has violated this policy, another school district policy, or the law.

C. An individual investigation or search will be conducted if school authorities have reasonable suspicion that the search will uncover a violation of law or school district policy.

D. Parents have the right at any time to investigate or review the contents of their child's files and e-mail files. Parents have the right to request the termination of their child's individual account at any time.

E. School district employees should be aware that the school district retains the right at any time to investigate or review the contents of their files and e-mail files. In addition, school district employees should be aware that data and other materials in files maintained on the school district system may be subject to review, disclosure or discovery under Minnesota Statutes, Chapter 13 (the Minnesota Government Data Practices Act).

F. The school district will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies conducted through the school district system.

XIII. INTERNET USE AGREEMENT

A. The proper use of the Internet, and the educational value to be gained from proper Internet use is the joint responsibility of students, parents and employees of the school district.

B. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a school account or resource to access the Internet.

C. The Internet Use Agreement form for students must be read and signed by the user, the parent or guardian, and the supervising teacher. The Internet Use Agreement form for employees must be signed by the employee and then be filed in the school district office.

XIV. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the school district system is at the user's own risk. The system is provided on an "as is, as available" basis. The school district will not be responsible for any damage users may suffer, including, but not limited to, loss, damage or unavailability of data stored on school district diskettes, tapes, hard drives or servers, or for delays of changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system or internet.

XV. USER NOTIFICATION

A. All users shall be notified of the school district policies relating to Internet use.

B. This notification shall include the following:

1. Notification that Internet use is subject to compliance with school district policies.

2. Disclaimers limiting the school district's liability relative to:

   a. Information stored on school district diskettes, hard drives or servers.
   b. Information retrieved through school district computers, networks or online resources.
   c. Personal property used to access school district computers, networks or online resources.
   d. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.

3. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.

4. Notifications that, even though the school district may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.

5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations that any financial obligation incurred by a student through the Internet or the sole responsibility of the student and/or the student's parents.

6. Notification that the collection, creation, reception, maintenance and dissemination of data via the Internet, including electronic communications, is governed by Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Pupil Records.

7. Notification that, should the user violate the school district's acceptable use policy, the user's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.

8. Notification that all provisions of the acceptable use policy are subordinate to local, state and federal laws.

XVI. PARENTS' RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

A. Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies and other possibly offensive media. Parents are responsible for

monitoring their student's use of the school district system and of the Internet if the student is accessing the school district system from home or a remote location.

B. Parents will be notified that their students will be using school district resources/accounts to access the Internet and that the school district will provide parents the option to request alternative activities not requiring Internet access.

This notification should include:

1. A copy of the user notification form provided to the student user.

2. A description of parent/guardian responsibilities.

3. A notification that the parents have the option to request alternative educational activities not requiring Internet access and the material to exercise this option.

4. A statement that the Internet Use Agreement must be signed by the user, the parent or guardian, and the supervising teacher prior to the use by the student.

5. A statement that the school district's acceptable use policy is available for parental review.

XVII. IMPLEMENTATION; POLICY REVIEW

A. The school district administration may develop appropriate user notification forms, guidelines and procedures necessary to implement this policy for submission to the school board for approval. Upon approval by the school board, such guidelines, forms and procedures shall be an addendum to this policy.

B. The administration shall revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.

C. The school district Internet policies and procedures are available for review by all parents, guardians, staff and members of the community.

D. Because of the rapid changes in the development of the Internet, the school board shall conduct an annual review of this policy.

Legal References: 15 U.S.C § 6501 *et seq.* (Children's Online Privacy Protection Act)
17 U.S.C § 101 *et seq.* (Copyrights)
20 U.S.C § 6751 *et seq.* (Enhancing Education through Technology Act of 2001)
47 U.S.C § 254 *et seq.* (Children's Internet Protection Act of 2000 (CIPA))
47 C.F.R. § 54.520 *(FCC rules implementing CIPA)*
Minn. Stat. § 125B.15 (Internet Access for Students)

Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Act)
Tinker c. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 89 S.Ct.733,21 L.Ed.2d 731 (1969)
United States v. American Library Association, 539 U.S. 194, 123 S.Ct. 2297, 56 L.Ed.2d 221 (2003)
Layshock v. Hermitage Sch. Dist., 412 F.Supp. 2d 502 (2006)
J.S. v. Bethlehem Area Sch. Dist., 807 A.2d 847 (Pa. 2002)

Cross References:

MSBA/MASA Model Policy 403 (Discipline, Suspension, and Dismissal of School District Employees)
MSBA/MASA Model Policy 406 (Public and Private Personnel Data)
MSBA/MASA Model Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)
MSBA/MASA Model Policy 506 (Student Discipline)
MSBA/MASA Model Policy 515 (Protection and Privacy of Pupil Records
MSBA/MASA Model Policy 519 (Interviews of Students by Outside Agencies)
MSBA/MASA Model Policy 521 (Student Disability Nondiscrimination
MSBA/MASA Model Policy 522 (Student Sex Nondiscrimination)
MSBA/MASA Model Policy 603 (Curriculum Development)
MSBA/MASA Model Policy 604 (Instructional Curriculum)
MSBA/MASA Model Policy 806 (Crisis Management Policy)
MSBA/MASA Model Policy 904 (Distribution of Materials on School District Policy by Nonschool Persons)