DRAFT: December 2011

Merrillville Schools

RESPONSIBLE USE OF MCSC TECHNOLOGY

1. Statement of MCSC Policy.

It is the policy of the Merrillville Community School Corporation to provide technical resources to students and employees for the purpose of promoting the efficient operations, advancing student achievement and allowing students and staff to master 21st century skills. MCSC expects staff and students to utilize the opportunities and facilities provided in a manner consistent with this policy.

2. Scope of this Policy.

This Policy applies to all technology provided by MCSC as well as the personal devices of students and employees (collectively "Users"). This includes, but is not limited to telephones, cell phones, digital media players, PDAs, laptop and desktop computers and work stations, direct radio communication, pagers, Internet access, voice mail, e-mail, text messaging, facsimile transmission and receipt, and any computer based research and/ or communication.

3. Definition of Terms Used in this Policy.

As used in this Policy**:**

"Confidential information" means information that is declared or permitted to be treated as confidential by state or federal law or Board Policy on access to public records.

"Proprietary information" means information in which a person or entity has a recognized property interest such as a copyright.

"Personal device" includes cell phones, smart phones, laptops, slates, handhelds or any other device that is not the property of MCSC but is used at school or a school activity, or connected to MCSC technology by a wired or wireless link.

"System Administrator" means MCSC employee designated by the Superintendent to maintain and/or operate MCSC's technology and network, and includes assistant System Administrator designated by the System Administrator appointed by the Superintendent.

"Technology" means computers and computer systems, public and private networks such as the Internet, phone networks, cable networks, voice mail, e-mail, telephone systems, copiers, fax machines, audio-visual systems, cell phones, PDA's, laptop & desktop computers, direct radio communications, pagers, text messaging, and similar equipment as may become available.

"User" means a MCSC employee, student, volunteer or other person authorized to use MCSC technology.

4. Violation of this Policy.

a. Intentional, knowing, and reckless or negligent violations of this Policy may result in denial of further access to technology, suspension or expulsion of students, and discipline of employees including suspension without pay or termination of employment. Such a violation by a person affiliated with a contractor or subcontractor rendering services to MCSC may result in cancellation of the contract of the contractor or sub-contractor.

b. A user observing or learning of a violation of this policy is required to report the violation of this Policy to the user's immediate supervisor (for employees or volunteers), or teacher (for students).

5. Ownership of MCSC Technology & Information.

a. The technology provided by MCSC and all information stored by that technology is at all times the property of MCSC, subject to the copyright interest of an author. Documents and other works created or stored on MCSC technology are the property of MCSC and are not the private property of the user. This includes all information created using technology and/or placed on a website, blog and/or other storage device.

b. A user's history of use and all data stored on or sent to or from MCSC technology shall at all times be subject to inspection by the System Administrator or a designee without notice to the user before of after the inspection. The System Administrator may deny, revoke, or suspend a user's accounts and/or access to MCSC technology.

c. Before being given access to MCSC technology, each user shall be required to agree that they have read, understand, and agree to be bound by the following standards and condition for responsible use of that technology:

1. They will comply with all conditions for the responsible use of MCSC technology established by MCSC, System Administrator, or Superintendent.

2. They will notify a System Administrator if they have violated the conditions established for the use of MCSC technology or have witnessed or become aware of another user misusing MCSC technology. Users shall be responsible for noting and reporting any inappropriate use of MCSC technology in violation of MCSC policy or conduct standards including threats, bullying, harassment, or communications proposing or constituting a violation of the law or the Student Code of Conduct.

3. They shall not have an expectation of privacy in any use of MCSC technology or the content of any communication using that technology other than a live telephone call, and the System Administrator or a designee may monitor their use of technology without notice to them, and examine all system activities the user participates in including but not limited to, e-mail, recorded voice and video transmissions, to ensure proper and responsible use of MCSC's technology. Monitoring shall include the use of voice-mail but shall not include monitoring a live communication between two or more parties unless at least one user is aware of the monitoring.

4. The user's history of use and any information or document accessed or stored on MCSC technology is subject to inspection by the System Administrator or a designee and is subject to production pursuant to the Indiana Access to Public Records Act, Ind. Code 5-14-3, subject to the decision of the System Administrator or Superintendent to claim a permissive or mandatory exemption to disclosure under that statute.

5. They shall not have an expectation that data in any form created, maintained, transmitted or stored in or on MCSC technology will be maintained for any specific period of time, protected from unauthorized access, or deleted from the system or storage when the user deletes the information from their account.

6. If they make use of a password, code or encryption device to restrict or inhibit access to electronic mail or files, they will provide access to that information when requested to do so only by the user's supervisor or the System Administrator. This includes personal technology brought to or accessed during the work or student day or at a school activity including bus transportation.

The System Administrator or a designee shall be authorized to override any password or encryption device to access the technology.

7. A user's information stored on MCSC technology will not be stored beyond student graduation or employee separation.

6. Investigation of Potential Violations of this Policy.

a. **Students**. If a System Administrator has reasonable cause to believe a student has violated this policy or additional rules promulgated by the System Administrator and approved by the Superintendent, the System Administrator or a designee may investigate to determine if a violation has occurred. The results of the investigation shall be reported to the System Administrator by e-mail or in person, and the System Administrator shall take appropriate action.

b. **Employees & Volunteers**. If a System Administrator has reasonable cause to believe an employee or volunteer has violated this policy or additional rules promulgated by the System Administrator and approved by the Superintendent, the System Administrator or a designee may investigate to determine if a violation has occurred. If the investigation is not done by a System Administrator, the results of the investigation shall be reported to a System Administrator by e-mail or in person, and the System Administrator shall take appropriate action.

c. **Appeals**. A decision by a System Administrator in response to an investigated allegation of a violation this policy or additional rules promulgated by the System Administrator and approved by the Superintendent may be appealed in writing to the Superintendent whose decision concerning continued access to MCSC technology and any other penalty shall be final.

7. Standards for Responsible Use of Technology.

a. MCSC believes that technology users have the same responsibilities while using MCSC technology that are expected in any other school activity. Responsible use of technology is ethical, academically honest, respectful of the rights of others, and consistent with MCSC's mission. Technology should be used by students to learn and communicate in correlation with the curriculum while under a teacher or supervisor's direction. Student owned personal devices and MCSC technology shall be used by students under teacher supervision with the objective of improving instruction and student learning.

b. Users must respect and protect the privacy intellectual property rights of others and the principles of their school community.

c. The privilege of use of MCSC technology access comes with personal responsibilities for each user. Access is not a right and is provided on the condition that the user complies with this policy and any additional rules promulgated by the System Administrator and approved by the Superintendent. Use of MCSC or personal devices or MCSC technology on school property or for school purposes must be consistent with the educational mission and objectives of MCSC. Misuse of MCSC technology may result in sanctions and civil and criminal penalties.

d. The System Administrator is authorized to select, adopt and endorse the use of specific web based resources for teacher and student use. This may include resources for web site creation, multimedia projects, presentations, and other collaborations. The System Administrator in consultation with the Superintendent's other designees will select resources based upon online safety, coordinated professional development, and informed technical support. If a teacher or student desires to use an alternate resource, they may make request to the System Administrator via the established waiver

process.

e. Any recording made on school grounds without written permission of a System Administrator is subject to copyright laws and the protection of the privacy right of others, including personally identifiable information about a student protected by the Family Education Rights and Privacy Act ("FERPA"). Any recording, data, or image in violation of this standard may be confiscated and deleted by the System Administrator. Any use of a personal recording device to invade the privacy of another person will result in sanctions for the person making the recording.

8. **Conditions & Standards for Responsible Student Use of MCSC Technology.**
The following apply to all student use of MCSC technology:

a. Creation of a web user ID by a student must be under the supervision of a teacher for the purpose of an assignment.

b. Students shall not be required to divulge personal information for access to a non-district managed technology.

c. Students will be permitted access to the Internet through MCSC technology unless a parent/guardian has signed and returned a "Student Electronic Resources Restriction Form" within the preceding twelve (12) months.

d. Student use shall be filtered to minimize access to inappropriate materials. Student access to inappropriate materials despite the presence of the filter shall be reported immediately to the System Administrator. The filtering software shall not be disabled or circumvented without the written authorization of a System Administrator.

e. Monitoring of Internet access by the designees of a System Administrator should be expected by users. However, there is no guarantee that all student access will be monitored.

f. While online, student users should not reveal personal information such as name, age, gender, home address or telephone number, and are encouraged not to respond to unsolicited online contacts and to report to a teacher or supervisor any online contacts which are frightening, threatening, or otherwise inappropriate.

g. Students, parents and staff are advised that any student connection to any Internet or network provider not under MCSC control may not be properly filtered, at least to the same degree as connection through MCSC provided access. MCSC is not responsible for the consequences of access to sites or information through resources that circumvent MCSC's filtering software.

9. Conditions & Standards for Responsible Use of MCSC Technology Applicable to All User's.
The following apply to all users of MCSC technology including students, employees, and volunteers:

a. Users will demonstrate legal and ethical behavior at all times when using MCSC technology.

b. Users will become familiar with and follow all laws, including copyright laws and fair use guidelines.

c. Users will become familiar with and comply with all expectations of MCSC for the responsible use of MCSC technology as communicated in school handbooks, school board policy, and other communications and standards concerning the use of MCSC technology.

d. Users accessing the Internet through personal devices connected to MCSC technology must comply with this policy.

e. Users connecting personal devices to MCSC technology do so at their own risk. MCSC is not responsible for damages to hardware or software as a result of the connection of personal devices to MCSC technology.

f. Users should not knowingly transmit a computer virus or other malware that is known by the user to have the capability to damage or impair the operation of MCSC technology, or the technology of another person, provider, or organization.
The Superintendent is authorized to develop administrative guidelines further refining what communication is related to MCSC business.

10. Protection of Proprietary and Confidential Information Communicated or Stored on MCSC Technology.

a. Users of MCSC's technology are expected to protect the integrity of data, personal privacy, and property rights of other persons when using MCSC technology. "Confidential information" as used in this Policy is information declared confidential by MCSC's Policy on Access to Public Records or state or federal law. Confidential information should never be transmitted or forwarded to or through a person not authorized to receive the information.

b. Any user communicating using MCSC technology shall be responsible for knowing what information is confidential under law or MCSC policy, and the transmission of confidential information in error may result in discipline of the user transmitting the confidential information.

c. The practice of using distribution lists to send information shall not excuse the erroneous disclosure of confidential information. Users shall determine that distribution lists are current and review each name on any list before sending confidential information including but not limited to personally identifiable information about students protected by the Family Educational Rights and Privacy Act ("FERPA").

d. Users should not access confidential information in the presence of others who do not have authorization to have access to the information. Confidential information should not be left visible on the monitor when a user is away from the monitor.

e. Users should not copy, file share, install or distribute any copyrighted material such as software, database files, documentations, articles, music, video, graphic files, and other information, unless the user has confirmed in advance that MCSC has a license permitting copying, sharing, installation, or distribution of the material from the copyright owner. Violation of the right of a copyright owner will result in discipline of a student or employee, and may subject the violator to civil and criminal penalties.

11. **Security of MCSC Technology.**

a. Security on any MCSC technology is a high priority when the resource involves many users and contains proprietary and confidential information. A user shall immediately notify the System Administrator if a security issue is identified. A security issue shall not to be disclosed or demonstrated to other users except in the presence of the System Administrator or a designee.

b. A user shall never use another user's password, or account, even with the permission from the user. Any need to have access to another user's account should be addressed to the System Administrator or a designee.

c. An unauthorized attempt to log on to MCSC technology as a System Administrator will result in cancellation of the user's access to MCSC technology and may result in more severe discipline including termination for employees and expulsion for students.

d. A user identified as a security risk based upon one or more violations of this Policy may be denied access to all MCSC technology. A decision denying or restricting a user's access may be appealed in writing to the Superintendent or a designee within ten (10) calendar days after written notice of the System Administrator's decision to the user. The decision of the Superintendent shall be final.

12. Incurring Fees for Services.

No user shall allow charges or fees for services or access to a database to be charged to MCSC except as specifically authorized in advance of the use by a System Administrator. A fee or charge mistakenly incurred shall be immediately reported to the System Administrator. Incurring fees or charges for services to be paid by MCSC for personal use or without prior authorization of the System Administrator may result in discipline including suspension or expulsion of a student, or suspension without pay or termination of an employee.

Staff and Students may also be asked to comply with their schools specific Technical Use Policy, Code of Conduct and Dress Code as they relate to technology and use.

Student Electronic Resources Restriction Form

Name of School: _____

Name of Student: _____Date of Birth: _____ (Please Print)

I/We direct that the child named above not be permitted to access the Internet using MCSC resources for the _____ school year.

Signature of Parent(s)/Guardian: _____ Date: _____

Note: Return this form to the Principal of your child's school ONLY if you do NOT want Internet access for your child. In situations where other students will be accessing the Internet your child will be provided alternative resources. Return of this form does not prohibit your child's teacher(s) from accessing the Internet in your child's presence. The restriction implemented by this form expires on July 1 of each school year and must be renewed for each subsequent school year.