EMPLOYEE ACCEPTABLE USE TECHNOLOGY POLICY

1.0 PURPOSE

1.1 Communications and computer technology at MSD Decatur Township are provided and maintained for instructional, educational, and administrative purposes only. The following guidelines implement Board policy, Employee Use of Technology, and govern the use of these technologies by employees during the performance of their duties. Use of the district's computing resources is a privilege, not a right.

2.0 Access to Technology Equipment and Services

2.1 Access to technology is provided to facilitate the instructional and administrative tasks performed by district employees and volunteers. The level of access provided will coincide with the requirements of each employee's job duties and/or responsibilities.

2.2 Computer files and communications over electronic networks, including e-mail, voice mail and Internet access, are not private. This technology should not be used to transmit confidential information about students, employees, or district business.

2.3 To ensure proper use, the Superintendent/designee may monitor the district's technological resources, including e-mail, voice mail systems and Internet usage, at any time without advance notice or consent.

3.0 Acceptable Use

3.1 It is a general policy that online communication is to be used in a responsible, efficient, ethical, and legal manner in support of education, business and/or research and within the educational program and goals of the MSD Decatur Township. The use of electronic information resources is a privilege, not a right. Each user is always personally responsible for this provision when using electronic information services.

3.2 Site administrators, building administrators, or department heads may set more restrictive guidelines for employees in their area of responsibility.

3.3 While electronic information resources offer tremendous opportunities of educational value, they also offer persons with illegal or unethical purposes an avenue for reaching students, teachers, and others, including parents. MSD Decatur Township does not have control of the information on commercial electronic information services or the information on the Internet, although it attempts to provide prudent and available barriers. Sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate, or potentially offensive to some people.

3.4 Should an employee see any unacceptable materials or inappropriate use, he/she shall notify the site administrator or supervisor immediately. Report any instances where the Acceptable Use Policy or security may be violated. Report inappropriate Internet Web sites to the district Technology Department so that access to the sites can be blocked in the future.

3.5 If there is any doubt as to the appropriate use of a district-provided electronic system, review the use in advance with a supervisor and/or a member of the Technology Department.

4.0 Proper Use and Care

4.1 Before operating any equipment, users will be made familiar with the basics of safety and damage prevention and trained on proper care and operation. Users will be assessed to determine their technical capabilities and will be properly trained and supported by the Technology Department, as systems are issued for their use.

4.2 In some cases, specific software is used to protect essential system configurations, requiring each user of shared systems to log-on individually, and enabling only the services for which the user is authorized.

4.3   Equipment abuses are unacceptable whether out of frustration, misuse, negligence or carelessness. Users are responsible for damage to or loss of district equipment. District vandalism policies apply, making users liable for intentionally inflicted damage.

4.4   Users should not attempt repairs without authorization or support from designated district or school site personnel. Volunteers – students, parents, family members, or friends – are not authorized to attempt repairs on district equipment.

4.5   Guidelines for the care and use of computer software are like hardware policies. Users are responsible for damage to or loss of district software systems. District vandalism policies apply to software as well, making users liable for intentionally inflicted damage.

4.6   Users shall not install or modify applications without approval and support of the district Technology Department. Any unauthorized changes to systems, operating software, application software, or hardware configurations will be reversed by technology or instructional staff. File-sharing software cannot be installed or used on district computers for the purpose of illegally sharing copyrighted materials such as music, images, and software. This type of software is often used to "pirate", or illegally copy, music across the Internet. These Napster-like software packages are distributed under many different names including Gnutella, WinMX, Kazaa, LimeWire, Morpheus, and others. The use of this type of software is illegal when used to share copyrighted material. The most common use is the illegal "swapping" of music encoded in the MP3 format and is a violation of U.S. copyright laws.

4.7   Users shall not download or install copyrighted software without Technology Department approval. Non-licensed software will not be installed.

4.8   Copyrighted material shall be posted online only in accordance with applicable copyright laws.

4.9   To ensure proper configuration and to safeguard network security and performance, users should not attach computers, printers, network equipment (including wireless access points), or other types of hardware to the district's network without prior approval and support of the Technology Department. Attaching personally owned technology equipment to district hardware or to the district network is not allowed. Any equipment found to be in violation of this policy will be immediately disconnected.

5.0   Personal Responsibility

5.1   All technology equipment is district property and is provided for instructional or administrative use only. Personal use is limited in the same manner as other similar district property. Supervisors will provide guidance as to the appropriate level of personal use.

5.2   Employees shall not access, post, submit, publish, email, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs.

5.3   Employees shall not use district technology systems to promote unethical practices, or any activity prohibited by law, Board policy, or administrative regulations.

5.4   Employees shall not use the system to engage in commercial or other for-profit activities without permission of the Superintendent or designee. In addition, district electronic resources cannot be used to conduct political or religious activities. District e-mail cannot be used to advertise or solicit for non-district sponsored events, activities, or organizations.

5.5   The district maintains a public Internet site and an in-house Intranet site. All materials published on these sites must follow the same Board Policies and Education Code Sections that apply to printed material. These policies include restrictions on the content, nature, purpose, and volume of information to be published. Intranet pages are provided for district employees and students only. Any information to be posted on the public Web site or in-house Intranet site must be

approved through the district technology department (or their designee) and the district's Communications Department. Principals or designee must approve all postings on school web sites. Restrictions apply to links to other sites that may not be appropriate and to personal information or pictures of students whose parents have not provided consent for their use. Specific Web site guidelines are established and available through the district's Communications Department.

5.6 Do not store personal files or applications on district media. Personal files will not be retained if it is necessary to reimage the computer system. Excessive use of approved district storage areas will be addressed on an individual basis.

5.7 Employees shall not attempt to interfere with other users' ability to send or receive email, nor shall they attempt to read, delete, copy, modify, or forge other users' email.

5.8 Employees shall not develop any classroom or work-related web sites, blogs, forums, or similar online communications representing the district or using district equipment or resources without permission from the district Technology Department. Such sites shall be subject to rules and guidelines established for district online publishing activities including, but not limited to, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs any such site shall include a disclaimer that the district is not responsible for the content of the messages. The district retains the right to delete material on any such online communications.

5.9 Users shall report any security problems or misuse of the services to the Superintendent or designee.

6.0 Security and Passwords

6.1 To maintain security, users are issued unique User ID's and passwords to enable their access. Do not use other people's passwords. Do not write down a password where others can see it, and change passwords regularly as recommended by Technology Department policies. Do not allow others to use your password for any reason. Confidential student information found in the student management system (Skyward) and other locations should not be accessible by students through a teacher login. The Superintendent and/or Technology Department administrator has access to any passwords used so he/she may have system access when the employee is absent or on leave. More information regarding the district "Password Protocol" can be found at: http://decatur.schoolfusion.us/ under the Technology Center webpage.

7.0 GPS Tracking Policy

7.1 Any district technology employee reserves the right to locate devices owned by the district. By agreeing to this policy, you consent to the use of your location data and services by the district for the purpose of, but not excluded to, loss and/or theft.

8.0 Penalties for Violation

8.1 Violation of the Acceptable Use Policy may result in a reduction or loss of access privileges. In many cases, access privileges may be essential to job functions. Additionally, those failing to follow the guidelines contained in this AUP may face disciplinary action in accordance with collective bargaining agreements, state law, and Board policy.

9.0 Employee Acknowledgment

9.1 All employees of MSD Decatur Township who have access to district technology will be required to annually acknowledge that they have received, read, and accepted this policy statement.

<u>EMPLOYEE ACKNOWLEDGEMENT</u>

I have received, read, and accept the guidelines in the Administrative Regulation on Employee Acceptable Use of Technology.

_____ _____ _____

Printed Name   Signature   Department/Building

_____

Date