

# Marshfield R-I School District

## Acceptable Use Policy

(Updated 6-20-2016)

### I.) Users

A. **Student Users** - No student will be given "privileged" access to the district's technology resources until the district receives a User Agreement signed by the student and the student's parent(s), guardian(s), or person(s) standing in the place of a parent. Students who do not have a User Agreement on file with the district may be granted permission to use the district technology by the superintendent or designee.

B. **Employee Users** - No employee will be given "privileged" access to the district's technology resources before the district has a signed User Agreement on file. Authorized employees may use the district's technology resources for reasonable, incidental personal purposes as long as the use does not violate any provision of district policy, regulation or procedure, hinder the use of the district's technology for the benefit of its students or waste district resources. Any use that jeopardizes the safety, security or usefulness of the district's technology is considered unreasonable. Any use that interferes with the effective and professional performance of the employee's job is considered unreasonable. Because computers are shared resources, it is not appropriate for an employee to access, view, display, store, print, or disseminate information via district resources, including e-mail or Internet access that students or other users could not access, view, display, store, print or disseminate, without authorization by the district.

C. **Board Member Users** - Members of the school Board may be granted user privileges, including a mail address, upon completion of a User Agreement. Board members will set an example of responsible use and will abide by District policies, regulations and procedures. Board members will comply with the Missouri Sunshine Law.

D. **External Users** - Consultants, counsel, independent contractors, and other persons having professional business with this school district may also be granted user privileges at the discretion of the Superintendent or Technology Coordinator, subject to completion of a User Agreement and for the sole, limited purpose of conducting business with the school. External users must abide by all laws, district policies, regulations and procedures.

### II.) Privacy

A user does not have a legal expectation of privacy in the user's electronic communications or other activities involving the district's technology resources. All district technology resources are considered district property. The district may maintain or improve technology resources at any time. The district may remove, change or exchange hardware or other technology between buildings, classrooms, employees, students or any other user at any time, without prior notice. Authorized district personnel may load or delete new programs or information, install new equipment, upgrade any system or enter any system to correct problems at any time. The district may examine all information stored on district technology resources at any time. The district may monitor employee and student technology usage. Electronic communications (email, instant messaging, etc.), all data stored on the district's technology resources, and downloaded material, including files deleted from a user's account, may be intercepted, accessed or searched by district administrators or designees at any time.

### III.) Violations of Technology Usage Policies and Procedures

Use of the district's technology resources is a privilege, not a right. A user's privileges may be suspended pending an investigation concerning use of the district's technology resources. Any violation of district policy, regulations or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges. The administration may use disciplinary measures to enforce district policy, regulations and procedures. Employees may be disciplined or terminated for violating the district's policies, regulations and procedures. Any attempted violation of district policy, regulations or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation.

### IV.) Damages

A. All damages incurred by the district due to the misuse of the district's technology resources, including the loss of property and staff time, may be charged to the user. District administrators have the authority to sign any criminal complaint regarding damage to district technology.

B. The school district does not warrant that the functions of the system will meet any specific requirements the user may have, or that it will be error-free or uninterrupted; nor shall it be liable for any direct, or indirect, incidental, or consequential damages (including lost data, information, damage to media, etc.) sustained or incurred in connection with the use, operation, or inability to use the system.

### V.) General Rules and Responsibilities

A. Using another person's user ID and/or password for any reason is prohibited.

B. Sharing one's user ID and/or password with any other person is prohibited.

C. Deleting, examining, copying or modifying files and/or data belonging to other users without their prior consent is prohibited.

- D. Mass consumption of technology resources that inhibits use by others is prohibited.
- E. Unless authorized by the district, non-educational Internet usage is prohibited.
- F. Making School District computing resources available to individuals not affiliated with the Marshfield R-I School District without approval of the administration and/or technology director is prohibited. This includes but is not limited to; wireless access points, direct connections of foreign equipment to the district's network and the sharing of district software.
- G. Using proxy servers or trying to bypass the District's Internet filtering in anyway is prohibited.
- H. Changes to the computer's operating system in any way is prohibited. This includes but is not limited to changing an IP address, changing display settings and changing any other computer settings.
- I. Connecting any non-district external device to the network such as a laptop, usb drive or router is prohibited.
- J. Use of district technology for soliciting, advertising, fund raising, commercial purposes or for financial gain is prohibited, unless authorized by the district.
- K. Users are required to obey all laws, including criminal, copyright, privacy, defamation and obscenity laws. The school district will render all reasonable assistance to local, state or federal officials for the investigation and prosecution of persons using district technology in violation of any law.
- L. Accessing, viewing or disseminating information using district resources, including e-mail or Internet access, that is pornographic, obscene, child pornography, harmful to minors, obscene to minors, libelous, pervasively indecent or vulgar, or advertising any product or service not permitted to minors is prohibited.
- M. Accessing, viewing or disseminating information on any product or service not permitted to minors is prohibited unless under the direction and supervision of district staff for curriculum-related purposes.
- N. Accessing, viewing or disseminating information using district resources, including e-mail or Internet access, that constitutes insulting or fighting words, the very expression of which injures or harasses other people (e.g. threats of violence, defamation of character or of a person's race, religion or ethnic origin); presents a clear and present likelihood that, because of their content or their manner of distribution, will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities; or will cause the commission of unlawful acts or the violation of lawful school regulations is prohibited.
- O. Any use that has the purpose or effect of discriminating or harassing any person or persons on the basis of race, color, religion, sex, national origin, ancestry, disability, age, pregnancy, or use of leave protected by the Family and Medical Leave Act or the violation of any person's rights under applicable laws is prohibited.
- P. Any unauthorized, deliberate, or negligent action that damages or disrupts technology, alters its normal performance or causes it to malfunction is prohibited, regardless of the location or the duration of the disruption.
- Q. Users may only use properly licensed software, audio or video media purchased by the district or approved for use by the district. Any other software must be approved by the district and installed by the district's technical staff. All users will adhere to the limitations of the district's technology licenses. Copying for home use is prohibited unless permitted by the district's license and approved by the district.
- R. Users are prohibited from uninstalling any software off of the district's computers unless authorized by the administration or technology staff.
- S. At no time will district technology or software be removed from the district premises, unless authorized by the district.
- T. All users will use the district's property as it was intended. Technology or technology hardware will not be lifted, moved or relocated without permission from an administrator. All users will be held accountable for any damage they cause to district technology resources.
- U. All damages incurred due to the misuse of the district's technology may be charged to the user. The district will hold all users accountable for the damage incurred and will seek both criminal and civil remedies, as necessary.

#### **VI.) Technology Security and Unauthorized Access**

All users shall immediately report any security problems or misuse of the district's technology resources to a Teacher, Administrator, or the Technology Coordinator. No person will be given access to district technology if he/she is considered a security risk by the Superintendent, Technology Coordinator, or designee.

- A. Use of district technology resources in attempting to gain or gaining unauthorized access to any technology system or the files of another is prohibited.
- B. Use of district technology to connect to other systems, in evasion of the physical limitations of the remote system, is prohibited.
- C. The unauthorized copying of system files is prohibited.
- D. Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any district technology are prohibited.
- E. Any attempts to secure a higher level of privilege on the technology resources without authorization are prohibited.
- F. The introduction of disruptive/destructive programs into a school computer, the network, or any external networks is prohibited. Including, but not limited to; computer "viruses," "hacking" tools, scripts, & logic bombs.
- G. Accessing Proxy servers for any reason without permission from the Technology Coordinator is prohibited.

- H. Any attempt to connect to other systems, in evasion of the district security systems, is prohibited.
- I. Any attempt to connect to district resources using equipment not approved by the technology coordinator is prohibited.

#### **VII.) Online Safety - Disclosure, Use, and Dissemination of Personal Information**

- A. All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet.
- B. Student users are prohibited from sharing personal information about themselves or others over the Internet, unless authorized by the district.
- C. Student users shall not agree to meet with someone they have met online without parental approval.
- D. A student user shall promptly disclose to his or her teacher or another school employee any message the user receives that is inappropriate or makes the user feel uncomfortable, in any way.
- E. Users shall receive or transmit communications using only district-approved and district managed communication systems. For example, users may not use web-based e-mail, messaging, videoconferencing or chat services, except in special cases where arrangements have been made in advance and approved by the district. Examples of approved services would include school gmail accounts for the staff and students.
- F. All district employees will abide by state and federal law, Board policies, and district rules when communicating information about personally identifiable students.
- G. Employees shall not transmit confidential student information using district technology, unless designated for that use. Employees will take precautions to prevent negligent disclosure of student information or student records.
- H. No curricular or non-curricular publication distributed using district technology will include the address, phone number or email address of any student without permission.
- I. The Marshfield R-I School District reserves the right to limit access to any materials designated by the administrators and/or Technology Coordinator.

#### **VIII.) Electronic Mail**

- A user is responsible for all e-mail originating from the user's ID or password.
- A. Forgery or attempted forgery of e-mail messages is prohibited.
- B. Unauthorized attempts to read, delete, copy or modify e-mail of other users are prohibited.
- C. All users must adhere to the same standards for communicating online that are expected in the classroom, and consistent with district policies, regulations and procedures.

#### **IX.) Exceptions**

Exceptions to district rules may be made for district employees or agents conducting an investigation of a use that potentially violates the law, district policies, regulations or procedures. Exceptions may also be made for technology administrators who need access to district technology resources to maintain the district's resources or examine and delete data stored on district computers as allowed by the district's retention policy. i.e. Each spring the servers are cleared of data so that they will have storage for the coming year.

#### **X.) Waiver**

Any user who believes he or she has a legitimate reason for using the district's technology in a manner that may violate any of the district's adopted policies, regulations and procedures may request a waiver from the Technology Coordinator and the building principal, superintendent, or designees. In making the decision to grant a waiver to a student, the administrator shall consider the purpose, age, maturity, and level of supervision involved.

#### **XI.) Exception of Terms and Conditions**

All terms and conditions as stated in this document are applicable to the Marshfield R-I School District. These terms and conditions reflect the entire agreement of the parties and supersede all prior oral or written agreements and understandings of the parties. These terms and conditions shall be governed and interpreted in accordance with the laws of the State of Missouri, and the United States of America.

#### **XII.) Violations and Discipline**

Discipline will be applied according to the severity of the offense. Administration shall judge the violation and authorize discipline accordingly. Disciplinary actions taken shall include, but are not limited to the following.

- A. Each violation of the AUP will have a written report of the incident submitted to the building administration explaining the violation.
- B. The offender shall have a conference with the building administrator.
- C. The parent(s)/guardian(s) of the student will be notified of the offense and the discipline to be carried out.
- D. Detention of a set number of days shall be assigned according to the severity of the offense.
- E. Internet and/or network connectivity shall be removed for a set number of days.
- F. Computer access shall be suspended or revoked.
- G. Local and/or state authorities will be contacted and shall be given a report of the incident.
- H. Employee disciplinary action shall be taken up to and including dismissal.