

EMPLOYEE TECHNOLOGY USAGE & INTERNET SAFETY POLICY AGREEMENT

The Warren County R-III School District's technology and Internet resources are provided for the purpose of maximizing the educational opportunities and achievement of its students. The intent of this policy is to outline safe and acceptable use of district technology and Internet resources by all users. Users must agree to follow the district's policies and procedures and must have a signed *User Agreement* on file with the district before they are allowed access to district technology and Internet resources. This agreement is renewed on a yearly basis for all users.

General Expectations and Regulations

A consistently high level of personal responsibility is expected of all users granted access to district technology and Internet resources. All users are expected to follow all policies, regulations, procedures and guidelines set forth by the district. Use of these resources is a privilege, not a right. No user will be given an ID, password, or other access to district technology if he or she is considered a security risk by the superintendent or designee. Any violation of district policy, regulations or procedures regarding technology usage including unauthorized access, "hacking", bullying or harassment of others may result in warnings, usage restrictions, discipline actions, and/or legal proceedings. Any attempt to violate the district's technology policies 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. All users of district technology and Internet resources must abide by MOREnet's acceptable use policy, which may be viewed at www.more.net/content/service-policies.

Definitions -

For the purposes of this policy the following terms are defined:

Technology Resources – Technologies, devices and resources used to access, process, store or communicate information. This definition includes, but is not limited to: computers, modems, printers, scanners, fax machines and transmissions, telephonic equipment, audio-visual equipment, Internet, electronic mail, electronic communications devices and services, multi-media resources, hardware and software.

User – Any person who is permitted by the district to utilize any portion of the district's technology resources including, but not limited to, students, employees, School Board members and agents of the school district.

User Identification (ID) – Any identifier that would allow a user access to the district's technology resources or to any program including, but not limited to, e-mail and Internet access.

Password – A unique word, phrase or combination of alphabetic, numeric and non-alphanumeric characters used to authenticate a user ID as belonging to a user.

Social networking - establishing, maintaining, posting to, or otherwise participating in an electronic community on websites, blogs, or through accounts on social networking sites, which allow users to create custom profiles; post pictures and text; blog or comment; publish videos, photos or photo albums; on-line applications or custom layouts.

Cell Phone – All portable devices that send or receive calls or text messages, that allows the retrieval of e-mail or provide access to the Internet.

Authorized Users

The district's technology resources may be used by authorized students, employees, School Board members and other persons such as consultants, legal counsel and independent contractors. All users must agree to follow the district's policies and procedures. Unless authorized by the superintendent or designee, all users must have a signed *User Agreement* on file with the district before they are allowed access to district technology resources.

Use of the district's technology resources is a privilege, not a right. No potential user will be given an ID, password or other access to district technology if he or she is considered a security risk by the superintendent or designee.

All district technology users should be aware of the following:

- All users granted access to the district's technology resources are expected to maintain a high level of professional and personal responsibility.

- Limited personal use of the district's technology resources by authorized employees is permitted to the extent that it does not impact job performance and does not include activities that violate any provision of district policies or procedures, hinder the use of the district's technology for the benefit of its students or waste district resources.
- If an employee witnesses a violation of the internet usage policy, the employee shall report the incident to their supervisor.
- If a student witnesses a violation of the internet usage policy, the student shall report the incident to the building principal.
- The district filters Internet content. This limits the Internet sites that can be accessed by all network computer users including students, teachers, administrators, other staff and visitors. Because e-rate funds are used to provide the district's Internet access, the district must comply with the Children's Internet Protection Act (CIPA) by using a CIPA compliant content filtering system. These limits do not provide a foolproof filter to limit access to controversial material and the district will not be liable for any damages as a result of accessing objectionable material.
- All electronic-based information technology activity, including email and Internet searches, are subject to monitoring by the district Technology Department and students and employees have no right of privacy in any such data. Any discovered computer activity including, but not limited to an email message or Internet search that deals with inappropriate or illegal activities will be reported to the appropriate authority. Personal information and personal data files from individuals suspected of committing a crime may also be turned over to investigators by administrators of the district. The district will comply with any search warrants including those issued under the USA Patriot Act of 2001 which targets terrorist offenses.
- Passwords are not to be used by unauthorized individuals. Individuals provided with system passwords will assume responsibility for the proper use of those passwords. If a student or staff member feels that there is a security problem on the network, misuse of a district password, or a compromised password should report the matter immediately to the Technology Director.
- All users must abide by existing state and federal laws regarding electronic communication, including accessing information without authorization, sharing passwords, or causing a system to malfunction. All users must abide by the terms of service and use for any online service as well as all district policies governing electronic data and electronic mail (email) retention.
- All software installed on district servers must be approved prior to installation by the Technology Department. Student projects posted on district servers must follow district guidelines for acceptable content. District policies on student publications will also extend to school-sponsored web publications.
- Use of online educational services, including social media services utilized by the district for educational purposes only, provide online forums for students and staff to use for instructional collaboration, communication, and document sharing and storage. User accounts are set up and maintained by the district whereby staff and students can access their accounts and communicate with groups both inside and outside of school. Students and staff are required to follow administrative guidelines and instructions for use and are subject to the terms of the Technology and Internet Usage Policy Agreement. Program training is required and provided through the Technology Department.
- Students or employees who engage in investigatory activities commonly described as "hacking" are subject to loss of privileges and district discipline, as well as the enforcement of any district policy, state and/or federal laws that may have been violated. Hacking may be described as the unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of the district, a business, or any other governmental agency obtained through unauthorized means.
- Students and employees are expected to abide by generally accepted rules of electronic network etiquette: be polite in all communications; use appropriate language; do not share personal information other than as required by the district; do not damage, disrupt or prohibit use of the network by others; assume all transmissions via the network are public.

Technology Administration

The Board directs the superintendent or designee to create procedures governing technology usage and to assign trained personnel to maintain the district's technology in a manner that will protect the district from liability and will protect confidential student and employee information retained on or accessible through district technology resources.

Administrators of computer resources may suspend access to and/or availability of the district's technology resources to diagnose and investigate network problems or potential violations of the law or district policies and procedures. 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 or users at any

time without prior notice. Authorized district personnel may install or remove new programs or information, install new equipment, upgrade any system or enter any system to correct problems at any time.

Closed Forum

The district's technology resources are not a public forum for expression of any kind and are to be considered a closed forum to the extent allowed by law. The district's webpage will provide information about the school district, but will not be used as an open forum.

All expressive activities involving district technology resources that students, parents/guardians and members of the public might reasonably perceive to bear the imprimatur of the district and that are designed to impart particular knowledge or skills to student participants and audiences are considered curricular publications. All curricular publications are subject to reasonable prior restraint, editing and deletion on behalf of the school district for legitimate pedagogical reasons. All other expressive activities involving the district's technology are subject to reasonable prior restraint and subject matter restrictions as allowed by law and Board policies.

The following activities and behavior are prohibited:

- Sharing your user ID and/or password with another person. The user is responsible for his or her account information and for actions taken by any person using his or her ID or password.
- Any attempt to capture, share, or use another user's login account information.
- Accessing, copying, sharing, deleting, or otherwise modifying the files and/or data belonging to other users.
- Any attempt, whether successful or unsuccessful, to interfere with the ability of others to utilize district technology.
- Use of district technology or any personally-owned device in an attempt to hack into or gain unauthorized access to any technology system or resource or to connect to other systems either inside or outside of the district
- Any attempt to alter a user account in any way without authorization.
- Any activity that damages or disrupts technology, alter its normal performance, creates a denial of service, or cause it to malfunction in any way, including mass consumption of technology resources that inhibits the use by others.
- Any activity intended to discriminate, attack, bully, harass, or otherwise harm other people or their work including participation in such activity off campus that creates a material disruption of school operations.
- Use of obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or otherwise inappropriate language or speech communicated through district technology resources, including participation in such activity off campus that creates a material disruption of school operations.
- Downloading, installing or running any type of software, shareware, freeware, audio/video media or other programs or systems not authorized by the school district.
- Violating the limitations of district-owned or personally-owned software licenses.
- Violating any copyright laws, including downloading, distributing or copying copyrighted software, music, videos or any type of copyrighted material.
- Using district technology resources to access, view, share, or distribute information or material that is pornographic, obscene, child pornography, harmful or obscene to minors, pervasively indecent or vulgar, or otherwise objectionable, including material that advertises any product or service not permitted to minors.
- Using district technology for any illegal activity or to access material that promotes or advocates illegal activity.
- Unauthorized viewing or use of any electronic information or data including restricted information.
- Using district technology resources for soliciting, advertising, non-district fund-raising, or commercial purposes or for financial gain.
- Use of web-based email, chat rooms, messaging, videoconferencing, or other forms of electronic communications not authorized by the district.
- Use of any type of removable media from outside the district on district equipment.

- Disclosing any personally identifiable information about yourself or others including but not limited to name, school, address, telephone numbers, email address, or other personal contact or family information.
- Contact by students with someone they have communicated with on-line without parental approval. Students shall promptly report any communication he or she receives that is inappropriate or makes the user feel uncomfortable in any way to a teacher or other school employee.
- Downloading, storing, relaying or running any game or entertainment software or game server software, including games that run inside of web browsers except for specific instructional purposes as authorized by the district.
- Accessing fee services without permission from an administrator. Users who access such services without permission are solely responsible for all charges incurred.
- Attempting in any way to bypass, weaken or disable any district security system or device including the web content filtering system.
- Utilizing or attempting to use any personally owned technology device, including but not limited to any wired or wireless equipment, media device or player, or software of any type in order to connect to any district technology resource without prior authorization of the Superintendent or designee.
- Removing or relocating any technology resource without permission from an administrator or Technology Department staff member. At no time shall any district technology resource be removed from the district's premises without prior authorization. All damages incurred due to the negligent or intentional misuse of the district's technology will be charged to the user.
- District employees should never send emails that disparage students, parents, patrons, other employees, a school or the district or that are otherwise inflammatory.

Consequences for violating the district's Technology and Internet Usage Policy will be enforced and include, but are not limited to: suspension of district network privileges; revocation of network privileges; suspension of computer and Internet access; revocation of computer and Internet access; school suspension; expulsion; employee disciplinary action up to and including dismissal; legal action to recover financial damages; criminal legal action.

Damages

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

No Warranty/No Endorsement

The district makes no warranties of any kind, whether expressed or implied, for the services, products or access it provides. The district's technology resources are available on an "as is, as available" basis.

The district is not responsible for loss of data, delays, non-deliveries, mis-deliveries or service interruptions. The district does not endorse the content nor guarantee the accuracy or quality of information obtained using the district's technology resources.

Employee Web Pages

All district employees must comply with the Internet Web Page Guidelines issued by the district in Procedure EHB-AP.

Social Networking

The district recognizes that social networking, including blogging, Facebook, Twitter, etc. can be effective methods of communication; however, there are potential consequences that can arise from an employee's failure to use discretion in such activities. All employee use of social networking sites shall be subject to the conditions established therein. Nothing in this policy shall prohibit employees from the use of approved educational websites if such sites are used solely for educational purposes.

All district employees must comply with Board Policy EHB governing Technology and Internet Usage. In addition, when utilizing social networking websites, all district employees are subject to the following guidelines:

- Employees are expected to maintain a high level of professional and personal responsibility.

- No employee shall post any district data, documents, photographs or other district owned or created information on any website.
- No employee shall post personally identifiable student information or student photos on any website without parent/guardian consent.
- No employee shall knowingly allow students access to the employee's personal social networking website or webpage that discusses or portrays sex, nudity, alcohol or drug use or other behaviors associated with the employee's private life that would be inappropriate to discuss with a student at school.
- No employee shall knowingly grant students access to any portion of the employee's personal social networking website or webpage that is not accessible to the general public.
- Access to social networking websites for district related purposes requires approval by the Director of Technology prior to access.
- Access of social networking websites for personal use on district equipment is prohibited.
- Use of social networking sites during work hours on personal electronic devices is prohibited and should not interfere with employees' job duties.
- The use of district owned equipment and internet access is subject to monitoring by the district technology staff and employees have no expectation of privacy in activities utilizing district owned equipment regardless of whether or not the use occurs during the hours of employment.
- Employees who maintain or post to social networking sites, whom identify themselves as employees of the district, are required to post a disclaimer that the opinions expressed by the employee are solely those of the author and do not represent the views of the district. Employees should not use the district's logos in any postings.
- On-line communication, including but not limited to blogs, are used primarily as learning tools, either as extensions of conversations and thinking outside of regular class time, or as the basics for beginning new classroom discussions. Whatever you post on a blog can be read by anyone and everyone on the Internet. Do not post anything that you would not want students, parents, your best friend, your worst enemy, or the district to read.
- Employees shall not use social networking websites to address personnel issues pertaining to district employees.
- Employees are responsible for reading, knowing and complying with the Terms of Service of social networking websites.
- Employees are required to obey all laws, including criminal, defamation, copyright and obscenity laws, as well as Board policies and regulations.

Employees who violate this policy may face discipline and/or termination, in accordance with district policies.

Cell Phone Use

The district expects all employees to use cell phones in a responsible manner that does not interfere with the employee's job duties. Employees who violate district policy and procedures regarding cell phone use may be disciplined, up to and including termination, and may be prohibited from possessing or using a cell phone while at work. Cell phones may not be used in any manner that would violate the district's policy on student-staff relations.

General Cell Phone Use

The district prohibits any employee cell phone use that interrupts or disrupts the performance of duties by the employee or otherwise interferes with district operations, as determined by the employee's supervisor. This prohibition applies regardless of whether the cell phone used is owned by the employee or provided by the district.

Supervision of students is a priority in the district, and employees who are responsible for supervising students must concentrate on that task at all times. Employees shall not use a cell phone when they are responsible for supervising students unless any of the following conditions occurs:

1. There is an emergency.
2. The use is necessary to the performance of an employment-related duty at that particular time and cannot be avoided.
3. The employee has received specific and direct permission from a supervisor. Supervisors shall limit such permission to unusual circumstances such as communication regarding a family birth or surgery.

4. Even when these conditions exist, the employee is responsible for obtaining assistance in adequately supervising students during the approved use so that students are supervised at all times.

Use in Vehicles

Regardless of other provisions of this policy, unless there is an emergency, employees shall not use cell phones when:

1. Driving district-provided vehicles.
2. Operating a vehicle in which a student is being transported on district property.
3. Supervising students who are entering or exiting a vehicle, crossing thoroughfares or otherwise safely reaching their destinations.

Even in emergency situations, employees should first take all possible safety precautions before using cell phones.

Use of District-Provided Cell Phones

The district may provide cell phones and service to some employees to assist them in carrying out their employment-related duties on and off district property. Use of a district-provided cell phone is a privilege. The superintendent or designee has sole discretion as to which employees will be provided cell phones and may recall any previously issued cell phone. Employees do not have any expectation of privacy in district-provided cell phones or any information stored on them, and such phones may be confiscated and searched at any time. Employees are expected to exercise reasonable care to protect district-provided cell phones from damage or theft and must report any such incidents immediately. The district may require employees to reimburse the district for any damage or theft that was the result of the employee's negligence. Users of district-provided cell phones must abide by any use limitations included in the district's service contract.

Personal Use of District-Provided Cell Phones

Personal use of district-provided cell phones is permissible as long as the use does not exceed the limits of the applicable plan. However, personal use of a cell phone is not permitted if the phone or service is paid for under E-Rate. An employee whose use exceeds plan limitations will be required to reimburse the district for all expenses beyond those covered by the plan and may have privileges suspended or revoked unless the employee can show that all use was for employment-related duties and the phone was not used for personal reasons.

Staff shall notify an administrator or supervisor immediately if they encounter any violation of the Technology and Internet Usage Policy. Questions concerning use of district technology and Internet resources should be addressed through an administrator or the Technology Director.

Record Retention

All district employees must comply with the procedures set forth in Board Policy EHBD- Record Retention and district Email Procedural Guidelines.

Please sign and return the accompanying form.

(Revised and Board Approved April, 2011)