



Warren County R-III Schools

302 Kuhl Avenue Warrenton, Missouri 63383-2198 p636-456-6901 f636-456-7687 www.warrencor3.org

TECHNOLOGY USAGE & INTERNET SAFETY POLICY

John D. Long, Ph.D.

Superintendent

longjd@warrencor3.k12.mo.us

Tom Jaeger, Ed.D.

Assistant Superintendent

jaegerk@warrencor3.k12.mo.us

Pam Frazier

Chief Financial Officer

frazierpj@warrencor3.k12.mo.us

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.

Internet Access - In accordance with CIPA (the Child Internet Protection Act), the district has filtering/blocking software in place to protect against access to content that is illegal, defamatory, obscene, child pornography, harmful to minors or otherwise potentially offensive. In addition, the district supervises and monitors the usage of technology and Internet resources, and logs the on-line activities of all users. Students are instructed in the appropriate and safe use of these resources. Any attempt to evade, weaken, or disable any district security system, including the district's firewall and filtering/blocking software, is a serious violation of district policy. Although such protection measures are in place, no system is foolproof and the district cannot guarantee that users will never access inappropriate materials using district resources. Any user who accidentally accesses inappropriate material should immediately close the connection and report it to a teacher or supervisor. Although district technology is provided for educational purposes, parents should be aware that there may be times when students may be browsing non-educational sites. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using online media and Internet resources. Therefore, we support and respect each family's right to decide whether or not to apply for access. Internet access services are provided by the Mo. Research and Education Network (MOREnet). 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.

Privacy – A user does not have a legal expectation of privacy in the user's electronic data, communications, or other activities involving district technology resources, including e-mail, Internet access, or network resources. By using the district's network and technology resources, all users are consenting to having their electronic files and communications and all other use monitored by the district. Electronic communications and all data stored or accessed on district technology and Internet resources, including downloaded material and deleted files, may be intercepted, accessed or searched by district administrators or designees at any time.

The district makes no warranty or guarantee of any kind, whether expressed or implied, regarding the technology services, products, or access it provides, nor does it endorse or guarantee the accuracy or quality of information obtained using district technology and Internet resources. The district employs full-time staff responsible for the district's technology and user administration. However, it does not warrant or guarantee equipment and system functionality and is not responsible for loss of data, delays, or service interruptions.

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.
- Student use of web-based email, chat rooms, messaging, videoconferencing, or other forms of electronic communications not authorized by the district.
- Student 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.

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

Please sign and return the accompanying form.

(Revised and Board Approved March, 2010)