Policy: 6320.1
Date: 1/1/08

Winona R-III School District
Computer Acceptable Use Policy

The Board of Education recognizes that it is important for students to have access to electronic-based research tools and master skills for their application toward learning, problem solving, and production of work, and presentation of information. The Board also recognizes that while these resources represent extraordinary learning opportunities and enriching educational materials, they also offer persons with illegal, immoral or inappropriate motives, avenues for reaching students, teachers, staff, parents/guardians and members of the community. Additionally, these resources present tempting opportunities for users to explore areas that are confidential, have restricted access, are inappropriate and are disruptive to the classroom or workplace. It is the purpose of the District policy and regulations to outline acceptable **student** and **employee** behavior with respect to the use of District technology and electronic resources.

Access to electronic research requires students and employees to maintain consistently high levels of personal responsibility. The existing rules found in the District's Behavioral Expectations Policy (Board Policy/Regulation 2610) as well as employee handbooks clearly apply to students and employees conducting electronic research or communication.

One fundamental need for acceptable student and employee use of District electronic resources is respect for, and protection of, password/account code security, as well as restricted databases, files, and information banks. Personal passwords/account codes may be created to protect students and employees utilizing electronic resources to conduct research or complete work.

These passwords/account codes shall not be shared with others; nor shall students or employees use another party's password except in the authorized maintenance and monitoring of the network. The maintenance of strict control of passwords/account codes protects employees and students from wrongful accusation of misuse of electronic resources or violation of District policy, state or federal law. **Students or employees who misuse electronic resources or who violate laws will be disciplined at a level appropriate to the seriousness of the misuse. Employee discipline will be dealt with on a case-by-case basis (i.e., job targets or letters of reprimand placed in file.)**

The use of District technology and electronic resources is a privilege, which may be revoked at any time. Staff and students are only allowed to conduct electronic network-based activities that are classroom or workplace related. Behaviors which shall result in revocation of access shall include, but will not be limited to: damage to or theft of system hardware or software; alteration of system hardware or software; placement of unlawful information, computer viruses or harmful programs on or through the computer system; entry into restricted information on systems or network files in violation of password/account code restriction; violation of other users' rights to privacy; unauthorized disclosure, use or dissemination of personal information regarding minors; using another person's name/password/account to send or receive messages on the network; and use of the network for personal gain, commercial purposes, or to engage in political activity.

Students and employees may not claim personal copyright privileges over files, data or materials developed in the scope of their employment, nor may students or employees use copyrighted materials without the permission of the copyright holder. The Internet allows users access to a wide variety of media. Even though it is possible to download most of these materials, students and staff shall not create or maintain archival copies of these materials unless the source indicates that the materials are in the public domain.

Access to electronic mail (E-mail) is a privilege and designed to assist students and employees in the acquisition of knowledge and in efficiently communicating with others. The District E-mail system, when established, is designed solely for educational and work related purposes. **E-mail files are subject to review by District and school personnel.** Chain letters, "chat rooms" or Multiple User Dimensions (MUDs) are not allowed, with the exception of those bulletin boards, blogs or "chat" groups that are created by teachers for specific instructional purposes or employees for specific work related communication.

Students or employees who engage in "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.

To the maximum extent permitted by law, students and employees are not permitted to obtain, download, view or otherwise gain access to "inappropriate matter," which includes materials that may be deemed inappropriate to minors, unlawful, abusive, obscene, pornographic, descriptive of destructive devices, or otherwise objectionable under current District policy or legal definitions.

The District and school administration reserve the right to remove files, limit or deny access, and refer staff or students violating the Board policy to appropriate authorities or for other disciplinary action.

The use of District technology and electronic resources is a privilege, not a right, and inappropriate use may result in the cancellation of those privileges. All staff members and students who receive a password/account code will participate in an orientation or training course regarding proper behavior and use of the network. The password/account code may be suspended or closed upon the finding of user misuse of the technology system or its resources.

Students and employees are expected to abide by the generally accepted rules of electronic network etiquette. These include, but are not limited to, the following:

1. System users are expected to be polite. They may not send abusive, insulting, harassing, or threatening messages to others.

2. System users are expected to use appropriate language; language that uses vulgarities or obscenities, libels others, or uses other inappropriate references is prohibited.

3. System users may not reveal their personal addresses, their telephone numbers or the addresses or telephone numbers of students, employees, or other individuals during E-mail transmissions.

4. System users may not use the District's electronic network in such a manner that would damage, disrupt, or prohibit the use of the network by other users.

5. System users should assume that all communications and information is public when transmitted via the network and may be viewed by other users. The system administrators may access and read E-mail on a random basis.

6. Use of the District's electronic network for unlawful purposes will not be tolerated and is prohibited.

While the District is providing access to electronic resources, it makes no warranties, whether expressed or implied, for these services. The District may not be held responsible for any damages including loss of data as a result of delays, non-delivery or service interruptions caused by the information system or the user's errors or omissions. The use or distribution of any information that is obtained through the information system is at the user's own risk. The District specifically denies any responsibility for the accuracy of information obtained through Internet services.

The Board recognizes that security on the District's electronic network is an extremely high priority. Security poses challenges for collective and individual users. Any intrusion into secure areas by those not permitted such privilege creates a risk for all users of the information system.

The account codes/passwords provided to each user are intended for the exclusive use of that person. Any problems, which arise from the user sharing his/her account code/password, are the responsibility of the account holder. Any misuse may result in the suspension or revocation of account privileges. The use of an account by someone other than the registered holder may be grounds for loss of access privileges to the information system.

Users are required to report immediately any abnormality in the system as soon as they observe it. Abnormalities should be reported to the classroom teacher or system administrator.

The District shall use filtering, blocking or other technology to protect students and staff from accessing Internet sites that contain visual depictions that are obscene, child pornography or harmful to minors. The District shall comply with the applicable provisions of the Children's Internet Protection Act (CIPA) and the Neighborhood Internet Protection Act (NCIPA).

Vandalism is defined as any malicious attempt to alter, harm, or destroy equipment or data of another user, the District information service, or the other networks that are connected to the Internet. This includes, but is not limited to the uploading or the creation of computer viruses, the alteration of data, or the theft of restricted information. Any vandalism of the District electronic network or technology system may result in the immediate loss of computer service, disciplinary action and, if appropriate, referral to law enforcement officials.

While not all unacceptable uses can be listed, this is a list of many common violations: (Faculty, staff and students)

1. Use of the network for, or in support of, any illegal purposes, including obscene or pornographic material.

2. Use of the network for soliciting or distributing information with the intent to incite violence, cause personal harm or bodily injury, or to harass or stalk another individual.

3. Non-educational uses including, but not limited to, games, discussion boards, chat rooms, instant messaging, wagering, gambling, junk mail, chain letters, jokes, private business activities, raffles, fundraisers, religious activities, or political lobbying/canvassing.

4. Using profanity, obscenity or language that is generally considered offensive or threatening to persons of a particular race, gender, religion, sexual orientation, or to persons with disabilities.

5. Plagiarizing any information gained on or through the network.

6. Using copyrighted materials, including commercial software, without permission of the copyright holder. When in doubt, contact teacher, administration or I.T. administrator.

7. Violating any provision of the Missouri School Student Act, which governs student's rights to privacy and the confidential maintenance of certain information including, but not limited to, a student's grades, test score, E-mail, etc.

8. Intentionally spreading computer viruses, spyware, or hacking programs.

9. **Sharing of log in names and/or passwords.**

10. Downloading any unauthorized software, games, programs, files, electronic media, and/or stand-alone applications from the internet.

11. Intentionally bypassing or instructing others on how to bypass internet filtering system of the district. Use of proxy sites such as clubsurfer.com is strictly prohibited.

12. Connecting to a modem to dial into any online service provider, or Internet Service Provider (ISP) or connect through a Digital Subscriber Line (DSL) while physically being connected to the Winona R-III Network where a T-3 line is functioning.

13. Intentionally disrupting the use of the Winona R-III Network or unlawful or illegal entry into an electronic system/software to gain secrets or private information.

14. Disclosing the contents of Winona R-III computer files, confidential documents, etc., to anyone other than an authorized representative.

15. Installation of MSN messenger, Kazza, or any peer-to-peer software, which can enable the user to copy or download copyrighted music or other materials.

16. Any action, which damages or disrupts the computer system, alters its normal performance, or causes it to malfunction.

All authorized users are to report promptly any breaches of security, or violations of acceptable use to their teacher or building principal. Authorized personnel will report such breaches to the I.T. Department as soon as possible. Failure to do so may result in discipline.

The Winona R-III Network is routinely monitored to maintain the efficiency of the system. Authorized users should be aware that their use of the network, including E-mail, is subject to reasonable and appropriate monitoring provided it follows state and federal laws.

In order to maintain an educational and operational computer network, the Winona R-III School District reserves the right to any of the following:

1. Student, faculty and staff access may be limited to a specified time because of the potentially large numbers of users who may need access to network and Internet resources as well as for personal productivity.

2. The District reserves the right to inspect the material stored in any location to which users have access and will edit and/or remove any material, considered objectionable by the district staff, found to be stored there.

3. Each user is limited to 20 Megabytes of server side storage space. Each user is responsible for managing this space as they see fit. If a user over fills their personal storage space, the district reserves the right to edit the contents, to reduce space used, at its discretion.

4. Internet access is provided primarily for educational purposes and the use of it for any other purposes may be limited at any time by district staff.

The District does not warrant that the functions of the system will meet any specific requirements you may have, or that it will be error free and uninterrupted; nor shall it be liable for any direct or indirect, incidental, or consequential damages (including lost data, information, or profits) sustained or incurred from the use, operation, or inability of a user to use the system.

The District will make a good faith effort to keep the network system and information accurate. However, users must acknowledge that there is no warranty of any kind, express or implied, regarding accuracy, quality, or validity of any data or information available. All authorized users holds the Board harmless from any claims, direct or indirect, incidental, or any damages arising from any use or inability to use the network, and from any claim for negligence in connection with the network. Use of the network is at the risk of the users.

I have read this policy and agree to adhere to the principles and procedures listed within. I understand that as a user I am solely responsible for my password and account. I also understand that additional rules and regulations may be added from time to time and that they become part of this agreement. Should I break this agreement, I understand that I may lose computer/internet privileges and will be disciplined according to the school handbook. I also understand that inappropriate or illegal use of computers and/or facilities could result in civil or criminal lawsuits. Parents and/or guardians may be held accountable for actions of their children.

Handbook Policy: 1st offense – 3 swats or 3 days Transition room and parent conference with principal
2nd offense – 5days in Transition room and parent conference with the Winona Board of Education
3rd offense – 5-10 day suspension from school

User Signature:____________________________________ Date:_____________________________

Parent/Guardian Signature:__________________________________ Date:_____________________________
(If user is under the age of 18)

User Grade Level:_________________ Teacher (1st hour):____

User Details (Please use Block Characters or Print clearly.)

First Name:_________________________ Middle Initial:__________ Last Name:___________________________

User Password:____
(6 characters or more, can use numbers and letters, **Keep this password secret**)

For the use of the Winona R-III School District Network Administration Staff only!

User Name:__________________________________ Account Number:____________________________________

Date Activated:_________________ Date Deleted:__________________ Expiration Date:___________________