ACCEPTABLE USE AND INTERNET SAFETY POLICY FOR THE COMPUTER NETWORK OF THE BUCYRUS CITY SCHOOL DISTRICT

The Bucyrus City School District is pleased to make available to students and staff access to interconnected computer systems within the District and to the Internet, the worldwide network that provides various means of accessing significant educational materials and opportunities.

In order for the school district to be able to continue to make its computer network and Internet access available, all users must take responsibility for appropriate and lawful use of this access. Users must understand that any misuse of the network and Internet access may jeopardize the ability of all users to enjoy such access. While the school's teachers and other staff will make reasonable efforts to supervise student use of network and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

Below is the Acceptable Use and Internet Safety Policy of the Bucyrus City School District. The policy is in addition to the Student Code of Conduct. Upon reviewing, signing, and returning this policy as the users have been directed, each user will be given the opportunity to enjoy Internet access at school and is agreeing to follow the policy. If a user is under eighteen (18) years of age, s/he must have his or her parents or guardians read and sign the policy. The Bucyrus City School District cannot provide access to any student who, if 18 or older, fails to sign and submit the policy to the school as directed or, if under eighteen (18), does not return the policy as directed with the signatures of the student and his/her parents or guardians.

Listed below are the provisions of your agreement regarding computer network and Internet use. If you have any questions about these provisions, you should contact the technology department, Central Office (419)562-4045, or the principal of your building. If any user violates this policy, the user's access will be denied, if not already provided, or withdrawn and s/he may be subject to additional disciplinary action.

A. PERSONAL RESPONSIBILITY

By signing this policy, you are agreeing not only to follow the rules in this policy, but are agreeing to report any misuse of the network to the technology department or Central Office, and/or your building principal (students must report offenses to the teacher) . Misuse means any violations of this policy or any other use that is not included in the policy, but has the effect of harming another or his or her property.

B. TERM OF THE PERMITTED USE

A user who submits to the school, as directed, a properly signed policy and follows the policy to which s/he has agreed will have computer network and Internet access during the course of the school year only. (Students: this is provided that you have not violated any classroom rules as well.) All users will be asked to sign a new policy each year during which they are students in or employed by the Bucyrus City School District before they are given an access account.

C. ACCEPTABLE USES

The Bucyrus City School District is providing access to its computer networks and the Internet for educational purposes only. If you have any doubt about whether a contemplated activity is educational, you may consult with the Central Office, building principal, or the technology department.

D. UNACCEPTABLE USES OF NETWORK.

Among the uses that are considered unacceptable and which constitute a violation of this policy are the following:

1. Uses that violate the law or encourage others to violate the law. Don't transmit offensive or harassing messages; offer for sale or use any substance the possession or use of which is prohibited by the school district's Student Discipline Policy; view, transmit or download pornographic materials or materials that encourage others to violate the law; intrude into the networks or computers of others; and download or transmit confidential, trade secret information, or copyrighted materials. Even if materials on the networks are not marked with the copyright symbol, you should assume that all materials are protected unless there is explicit permission on the materials to use them. Any use of copyrighted material on the network should uphold the standards and guidelines of educational fair use under Section 107 of H.R. 2223.
2. Uses that cause harm to others or damage to their property. For example, don't engage in defamation (harming another's reputation by lies); employ another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the Internet; upload a worm, virus, "trojan horse," "time bomb" or other harmful form of programming or vandalism; participate in "hacking" activities or any form of unauthorized access to other computers, networks, or information systems.
3. Uses that violate the conditions of the Ohio Revised Code dealing with students and employees rights to privacy.
4. Uses that jeopardize the security of users' access and of the computer network or other networks on the Internet. For example, don't disclose or share your password with others; don't impersonate another user.
5. Employees may not alter the settings that are placed on the computer including but not limited to: any settings found in the network properties or control panels that affect the performance of the computer or network. You may personalize the school district's computer equipment, except for programs that interfere with the performance and/or maintenance of the computer.
6. Uses that are commercial transactions. Users may not, for personal use or gain, buy or sell anything over the Internet. You should not give others private information about you or others, including credit card numbers and social security numbers.
7. Uses that disrupt the flow of data over the network.
8. Uses that encourage the use of drugs, alcohol, or tobacco. Nor shall they promote unethical practices or any activity prohibited by law or Board Regulation.
9. Downloading or using software that is harmful to the network and/or computer that you are using.
10. Do not take home, district equipment with out prior written consent from your building administrator and the central office (ask for a form to fill out). This includes Laptops. Laptops are expected to be used for school related projects and to be taken home only on a very temporary bases, and brought back the following school day. Laptops also need to be returned to the central office at the end of every school year to be inspected and updated.
11. The willful wasting of computer and networking facilities resources is considered inappropriate use. Wastefulness includes, but is not limited to, passing chain letters, generation of large volumes of unnecessary or non-work related printed output or disk space, or creation of heavy network traffic such as streaming radio or video for non-education purposes.

E. SOFTWARE

Computer software is protected by Federal copyright laws. Employees are prohibited from engaging in unauthorized duplication, distribution or alteration of any licensed software. Employees must abide by all software licensing agreements and may not illegally use or possess copyrighted software. Employees must not use software that they know has been illegally copied.

Network license software is typically used by a limited number of concurrent users. However, unless permitted by the license, this software must not be copied from the server to the employee's individual workstation or storage location.

Site license software can be used on any workstation at the site for which software is purchased. This software can be legally copied onto any site workstation that holds the license. However, unless permitted by the license, it must not be copied to workstations not owned by the license.
Single license software must not be copied to multiple machines or media in violation of the license agreement. However, employees may bring in personal single license software to install on the school's computer resources in the following circumstances: (also applies to all new software before it can be loaded on the machine)

1. The user can prove ownership (i.e. license agreement).
2. The user adheres to the licensing and copywriting agreements for the software.
3. The user has registered the software with the software company.
4. The user has completed the District Software Approval Form and has prior permission to install the software on the school's computer by the Central Office, Building Administrator, and district technology coordinator.

F. FILES STORED ON THE DISTRICT'S SERVER and/or ON THE DISTRICT'S COMPUTERS.

Files stored on the District's server must be for educational purposes only. No executable files or non-school related files are to be in an employee's folder. If such files are found on the server or on a District computer, they will be deleted immediately and the infraction will be reported. Files in an employee's folder are property of the District and may be reviewed without notification. When an employee leaves the District, all employee files will be deleted and the password will be revoked. Employees are expected to periodically clean files off of the server, including the e-mail server, and are to remove those files that are no longer necessary.

G. ETIQUETTE.

ALL users must abide by rules of network etiquette, which include the following:

1. Be polite. Use appropriate language. No swearing, vulgarities, suggestive, obscene, belligerent, or threatening language.
2. Avoid language and uses of language which may be offensive to other users. Don't use computer access to make, distribute, or redistribute jokes, stories, or other material, which is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation. Do not use profanity, obscenity, or other language that could be construed as harassment or disparagement of others based on their race, nationality, origin, citizenship status, sex, sexual orientation, age, disability, religion, or political beliefs.
3. Don't assume that a sender of e-mail is giving his or her permission for you to forward or redistribute the message to third parties or to give his/her e-mail address to third parties. This should only be done with permission or when you know that the individual would have no objection.
4. Be considerate when sending attachments with e-mail (where this is permitted). Be sure that the file is not too large to be accommodated by the recipient's system and is in a format, which the recipient can open.

H. INTERNET SAFETY

1. General Warning.

Individual Responsibility of Parents and Users. All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the computer network and Internet and stay away from these sites. If a user finds that other users are visiting offensive or harmful sites, s/he should report such use to the technology department or Central Office, and/or your administrator (students must report offenses to the teacher).

2. Personal Safety.

Be safe. In using the computer network and Internet, do not reveal personal information such as your home address or telephone number. Do not use your last name or any other information which might allow a person to locate you without first obtaining the permission of a supervising teacher. Do not arrange a face-to-face meeting with someone you "meet" on the computer network. Regardless of your age, you should never agree to meet a person you have only communicated with on the Internet in a secluded place or in a private setting.

3. "Hacking" and other illegal Activities.

It is a violation of this policy to use the Bucyrus City School's computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Employees are prohibited from negligently and/or intentionally damaging, destroying or altering school technology resources in any unauthorized or illegal manner (i.e., computer hacking, uploading/creating viruses, etc.) Any malicious attempt by an employee to harm or destroy data that is connected to the network is specifically prohibited. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.

4. Confidentiality of User Information.

Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and social security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by Ohio law, for internal administrative purposes or approved educational projects and activities.

Employees granted access to confidential records, of students or other employees, have the important responsibility of maintaining the confidentiality of information and may be discipline for sharing or releasing information to others without authorization. Information that is considered confidential should not be sent to a network printer without an authorized person available to safeguard its confidentiality during and after printing (i.e. pick it up from the network printer immediately don't print something if you can't get it at that time).

5. Active Restriction Measures.

The Bucyrus City School District, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering software or other technologies to prevent users from accessing sites that are obscene, contain pornography, child pornography, sites that may be harmful to minors, non-educational, and/or sites that adversely affect the computer network. The school will also monitor the online activities of users, through direct observation and/or technological means, to ensure that users are not accessing such depictions or any other material, which is inappropriate for minors. The term "harmful to minors" as used above means any picture, image, graphic image file, other visual depiction, words, group of words, or writings that

-taken as a whole or in part and with respect to minors, appeals to a prurient interest in nudity, or sex;

-depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; taken as a whole or in part, lacks serious literary, artistic, political, social, health, educational or scientific value as to minors. To abide by the rules laid out for us by the federal government we cannot allow anyone to use a "cell card" in their laptop / desktop or a web enabled phone on school grounds.

I. PRIVACY

Network and Internet access is provided as a tool for your education. The Bucyrus City School District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the Bucyrus City School District and no user shall have any expectation of privacy regarding such materials. The school district also reserves the right to search and seize computer resources used by employees, such as computers, disks, electronic mail messages, Internet materials, etc. The search will be conducted at the discretion of the school district, and the systems administrator will be involved in all searches.

J. FAILURE TO FOLLOW POLICY

The user's use of the computer network and Internet is a privilege, not a right. A user who violates this policy or a classroom computer policy (supplied by the teacher), shall at a minimum, have his/her access to the computer network and Internet disabled, which the school district may refuse to reinstate for the remainder of the user's enrollment/employment in the school district. A user violates this policy by his/her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this policy if s/he permits another to use his/her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. The school district may also take other disciplinary action in such circumstances.

K. WARRANTIES/INDEMNIFICATION

The Bucyrus City School District makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. It shall not be responsible for any claims, losses, damages, or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his/her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this policy. By signing this policy, users are taking full responsibility for his/her use, and the user who is eighteen (18) or older or, in the case of a user under eighteen (18), the parent(s) or guardian(s) are agreeing to indemnify and hold the school, the school district (Bucyrus City Schools), and the Data Acquisition Site that provides the computer and Internet access opportunity to the school district and all of their administrators, teachers, and staff harmless from any and all loss, costs, claims or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s) or guardian(s) agree to cooperate with the school in the event of the school initiating an investigation of a user's use of his or her access to its (the school's) computer network and the Internet, whether that use is on a school computer or on another computer outside the school district's network.

L. UPDATES

Users, and if appropriate, the user's parents/guardians, may be asked from time to time to provide new or additional registration and account information or to sign a new policy, for example, to reflect developments in the law or technology. Such information must be provided by the user (or his/her parents or guardian) or such new policy must be signed if the user wishes to continue to receive service. If after you have provided your account information, some or all of the information changes, you must notify the person designated by the school to receive such information.

ADOPTED: 12/03/1997: 03/25/2004 policy #7540.03
REVISED: 04/20/2005
Legal References: Children's Internet Protection Act of 2000 (H.R. 4577, P.L. 106-554)
Communications Act of 1934, as amended (47 U.S.C. 254[h], [l])
Elementary and Secondary Education Act of 1965, as amended (20 U.S.C.
6801 et seq., Part F)

This page Intentionally Left Blank

STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY AGREEMENT

To access Computers, e-mail, and/or the Internet at school, staff members must sign and return this form.

Use of the Internet is a privilege, not a right. The Board's Internet connection is provided for business, professional and educational purposes only. Unauthorized or inappropriate use will result in a cancellation of this privilege.

The Board has implemented the use of a Technology Protection Measures, which is a specific technology that will protect against (e.g., block/filter) Internet access to visual displays that are obscene, child pornography or harmful to minors. The Board also monitors online activity of staff members in an effort to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. () The Superintendent or Other Administrator may disable the Technology Protection Measure to enable access for bona fide research or other lawful purposes.

Staff members accessing the Internet through the Board's computers/network assume personal responsibility and liability, both civil and criminal, for unauthorized or inappropriate use of the Internet.

The Board reserves the right to monitor, review and inspect any directories, files and/or messages residing on or sent using the Board's computers/networks. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

( ) To the extent that a staff member has the proprietary rights to the design of a web site hosted on the Board's servers , the staff member agrees to license the use of the web site by the Board without further compensation.

Please complete the following information:

Staff Member's Full Name (please print):_____

School:_____

I have read and agree to abide by the Staff Network and Internet Acceptable Use and Safety Policy and Guidelines. I understand that any violation of the terms and conditions set forth in the Policy is inappropriate and may constitute a criminal offense. As a user of the Board's computers/network and the Internet, I agree to communicate over the Internet and the Network in an appropriate manner, honoring all relevant laws, restrictions and guidelines.

Staff Member's Signature:_____Date:____/____/____

The Superintendent is responsible for determining what is unauthorized or inappropriate use. The Superintendent may deny, revoke or suspend access to the Network/Internet to individuals who violate the Board's Staff Network and Internet Acceptable Use and Safety Policy and related Guidelines and take such other disciplinary action as is appropriate pursuant to the applicable collective bargaining agreement and/or Board Policy.

Sign and Return This Page ONLY