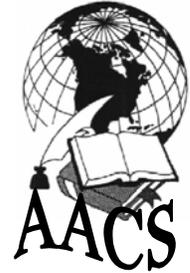


Acceptable Use and Internet Safety Policy

for the computer network of

Ashtabula Area City Schools

(Employees, volunteers, and other users)



Ashtabula Area City Schools is pleased to make available to students, employees, volunteers, and other users access to interconnected computer systems within the District and to the Internet, the world-wide 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 one user's 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 ("Policy") of the School District and for use of the Data Acquisition Site that provides Internet access to the School District. It is incumbent on the user to review this policy.

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 person that your School has designated as the one to whom you can direct your questions. If any user violates this Policy, the user's access will be denied, if not already provided, or withdrawn and he or she may be subject to additional disciplinary action.

I. PERSONAL RESPONSIBILITY

By utilizing district technology equipment, you are agreeing not only to follow the rules in this Policy, but are agreeing to report any misuse of the network to the person designated by the School for such reporting. 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.

II. TERM OF THE PERMITTED USE

All users will have computer network and Internet access during the course of the school year only. Non-compliance of the Acceptable Use Policy will result in disciplinary action.

III. ACCEPTABLE USES

- A. Educational Purposes Only.** The School District is providing access to its computer networks and the Internet for *only* educational purposes. If you have any doubt about whether a contemplated activity is educational, you may consult with the person(s) designated by the School to help you decide if a use is appropriate.
- B. 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.
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 jeopardize the security of user 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.
 4. uses that are commercial transactions. Students and other users may not sell or buy anything over the Internet. You should not give others private information about you or others, including credit card numbers and social security numbers.
- C. **Netiquette.** 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 which may be offensive to other users. Don’t use 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.
 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.

IV. INTERNET SAFETY

- A. **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. Parents of minors are the best guide to materials to shun. If a user finds that other users are visiting offensive or harmful sites, he or she should report such use to the person designated by the School.
- B. **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 real 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 or Internet without your parent’s permission (if you are under 18). 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.
- C. **“Hacking” and Other Illegal Activities.** It is a violation of this Policy to use the 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. 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.
- D. **Confidentiality of Student 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 or, if the student is 18 or over, the permission of the student himself/herself. 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.
- E. **Active Restriction Measures.** The School, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. 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. Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by

students age 17 and older. The term “harmful to minors” is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as meaning any picture, image, graphic image file, or other visual depiction that - taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; - 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, lacks serious literary, artistic, political, or scientific value as to minors.

V. PRIVACY

Network and Internet access is provided as a tool for your education. The 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 School District and no user shall have any expectation of privacy regarding such materials..

VI. 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, shall at a minimum, have his or her access to the computer network and Internet terminated, which the School District may refuse to reinstate for the remainder of the user’s time in the School District. A user violates this Policy by his or 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 he or she permits another to use his or 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.

VII. WARRANTIES/INDEMNIFICATION

The 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 or 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 or her use, and the user who is 18 or older or, in the case of a user under 18, the parent(s) or guardian(s) are agreeing to indemnify and hold the School, the School District, 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’s initiating an investigation of a user’s use of his or her access to its computer network and the Internet, whether that use is on a School computer or on another computer outside the School District's network.

Additional Guidelines for Staff, Volunteers, and Other Users

Staff, Volunteers, and Other Users are expected to:

1. Log out when not using the computers. No student is to use the computer under a Teacher/Volunteer/Other network user login.
2. Teacher/Volunteer/Other login and password information is never to be given to a student.
3. Downloads and Proxy Information

Users are to:

- a. Not download MP3 files or allow the download of MP3 files unless it is course of study related.
- b. Not remove or allow the removal or tampering of proxy server information.
- c. Not download or allow the download of internet browsers other than the one installed by the district.
- d. Download and/or install only programs approved by the district and/or principal

Examples

1. The free versions of Real Player and its components, Windows Media Player, and Adobe Acrobat Reader have been installed for educational use (Radio stations are not to be listened to on the computer). Updates should be downloaded when available.
2. Internet Chat programs, Napster, iMesh, and other MP3 programs may not be downloaded.
3. Programs are not to be brought from home and installed on the district computer equipment.

4. Monitor Student Use

- a. No student is to use computer equipment unsupervised.
- b. Students are to use computers for educational purposes only.
- c. Students are not to have access to email, chat rooms, or internet chat programs.
- d. Students are not to download or print without permission from the classroom teacher.

5. Only district purchased/approved computer equipment will be tied into the network.

Violations of the aforementioned guidelines, or any activity that compromises the integrity of the network, will result in the termination of network/internet access and/or possible disciplinary action.

Acceptable Use and Internet Safety Policy

Ashtabula Area City Schools is please to provide access to the Internet. The Internet is an electronic highway connecting hundreds of thousands of computers and millions of individual users all over the world. This computer technology will help propel our schools through the communication age by allowing students and staff to access and use resources from distant computers, communicate and collaborate with other individuals and groups around the world, and significantly expand their available information base. The Internet is a tool for lifelong learning.

Families should be aware that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive to some people. In addition, it is possible to purchase certain goods and services via the Internet which could result in unwanted financial obligations for which a student's parent or guardian would be liable.

While the District's intent is to make Internet access available in order to further educational goals and objectives, students may find ways to access other materials as well. Even with technical methods to regulate students' Internet access, those methods could not guarantee compliance with the District's Acceptable Use Policy. It is incumbent upon the user to comply with all aspects of the District's Acceptable Use Policy. The district may monitor computer activity either by direct observation and/or technological means.

The District believes that the benefits to students of access to the Internet and other technology used within the District exceed any disadvantages. Ultimately, however, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. Toward that end, the Ashtabula Area City Schools makes the District's complete Internet policy and procedures available on request for review by all parents, guardians, and other members of the community; and provides parents and guardians the option of requesting for their minor children alternative activities not requiring Internet use.

It is our belief that technology and Internet use are an integral part of our instructional methodology and is now part of our every day instruction.

If a parent wishes for a minor not to have access to the internet, the parent is to sign and return the required form requesting that the student not have access. It is incumbent upon the parent to confirm with the building principal that the form was received.

ADOPTED:

REVISED:

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)