

# Acceptable Use and Internet Safety Policy - (7540.03)

## 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 building principal. 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/her property.

## TERM OF THE PERMITTED USE

A student who submits to the school 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 will be asked to sign a new policy each year during which they are students in the School District before they are given an access account.

## ACCEPTABLE USES

- A. **Educational Purposes Only.** The 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 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. Students may not send or receive emails that contain inappropriate or obscene comments, suggestions, or language.
  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 student 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 Internet 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. Use of the network or school property to engage in cyberbullying is prohibited. Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm others.
  3. Don't assume that a sender of e-mail is giving his/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 systems and is in a format which the recipient can open.

## 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 students. Every user must take responsibility for his/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 student finds that other users are visiting offensive or harmful sites, s/he 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 scheduled 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.** Information that personally identifies an individual student may not be shared 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 students, through direct observation and/or technological means, to ensure that students 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:

1. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. 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;
3. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

## 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.

### **FAILURE TO FOLLOW POLICY**

The 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/her access to the computer network and Internet terminated, which the School District may refuse to reinstate for the remainder of the student's enrollment 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.

### **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/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 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/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.

### **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.

### **ADDITIONAL ITEMS OF CURRENT CONCERN FOR THE 1:1 IPAD INITIATIVE**

1. Students may only access their computer or network by using their assigned network account/password. Use of another person's account/password is prohibited. Students may not allow other Students to use their account/password. Students may not go beyond their authorized access. Students may not intentionally seek information or modify files, data, or passwords belonging to other users, or misrepresent other users on the computer/network.
2. Students may not use the network or school property to engage in illegal activities such as software pirating, peer-to-peer file sharing and/or intellectual property violations (ex: music, videos, books, television shows, movies, etc. which are under copyright).
3. While on the school network, use of chat clients, social networking sites, and personal web-based email are prohibited.
4. Use of non-educational games, videos, movies, or games/videos/movies not assigned by a teacher while on the network or using school property is prohibited.
5. When using the network or school computers, students must follow the directions of school teachers/staff and adhere to school policies.