

# **COMPUTER NETWORK AND INTERNET ACCEPTABLE USE POLICY AND AGREEMENT FOR STUDENTS OF THE LANCASTER CITY SCHOOL DISTRICT**

The District is pleased to provide our students with access to interconnected computer systems within the District and to the Internet via a worldwide network that provides various means of accessing significant educational materials and opportunities.

In order for the District to continue making its computer network and Internet access available, all students must take responsibility for appropriate and lawful use of this access. Students must understand that one student's misuse of the network and/or Internet access may jeopardize the ability of all students to enjoy such access. While teachers and other staff members will make reasonable efforts to supervise student use of network and Internet access, our employees must have student cooperation in exercising and promoting responsible use of this access.

The District recognizes the need to prevent students from accidentally or intentionally accessing inappropriate material via the Internet. To that end, the District has instituted the use of an Internet filter that prevents access to many sites that are known to violate the Lancaster City Schools' Acceptable Use Policy (AUP) and Internet Safety Policy. Filters are, however, imperfect devices and are not a reliable substitute for monitoring students' activities by their teachers and/or by other staff. Students should be guided to appropriate sites since neither the filter nor the inspection by our employees may prevent some students from reaching inappropriate material. All students under the age of 18 and their parent/guardian must sign the AUP before the student will be allowed network access. Personal Electronic Communications Equipment must also be used in accordance to this policy.

Upon reviewing, signing, and returning this Policy, each student will be given the opportunity to enjoy Internet access at school and will agree to follow the Policy. If a student is under 18 years of age, his/her parent/guardian must read and sign the policy. The 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 18, does not return the policy with the appropriate signatures of the student and his/her parent/guardian as directed.

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 your school principal or librarian. Either one will direct your questions to the appropriate person. If any student violates this policy, his/her access will be denied or withdrawn, and the student may be subject to additional disciplinary action.

## **I. Personal Responsibility**

By signing this policy, you are agreeing not only to follow the rules in this policy, but are also 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/her property.

## **II. Term Of The Permitted Use**

A student who submits a properly signed policy and who follows the policy to which he/she has agreed will have computer network and Internet access during the course of one school year only. Students will be asked to sign a new policy each school year before he/she will be given an access account.

## **III. Acceptable Uses**

A. Educational Purposes Only The District is providing access to its computer networks and to the Internet for only educational purposes. Personal Electronic Communications Equipment must be used in accordance to the student handbook and under the supervision of a staff member. 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.

- a) Don't transmit offensive or harassing messages.
- b) Don't offer for sale or use any substance the possession or use of which is prohibited by the District's Student Discipline Policy.
- c) Don't view, transmit or download pornographic materials or materials that encourage others to violate the law.
- d) Don't intrude into the networks or computers of others.
- e) Don't 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.

- a) Don't engage in defamation (harming another's reputation by lies).
- b) Don't 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.
- c) Don't upload a worm, a virus, a "Trojan Horse," a "time bomb" or any other harmful form of programming or vandalism.
- d) Don't participate in "hacking" activities or any form of unauthorized access to other computers, networks, or information systems.
- e) Do not download or install a program or software without permission from an authorized school official.

3) Uses that jeopardize the security of student access and of the computer network or other networks on the Internet.

- a) Don't disclose or share your password with others.
- b) Don't impersonate another user.

4) Uses that are commercial transactions. Students and other users may not sell or buy anything over the Internet nor use the computer and/or network for financial gain or illegal activity. 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 that may be offensive to other users. Don't use access to make, distribute, or redistribute jokes, stories, or other material that 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/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 be done only 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 that the recipient can open.
5. Note that electronic mail is not guaranteed to be private. People who operate the system do have access to all messages relating to or in support of illegal activities, and such activities will be reported to the proper authorities.

#### **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 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 guides to materials to shun. If a student finds that other users are visiting offensive or harmful sites, he/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 communicated with only 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 or materials that are (1) obscene, (2) pornographic 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 that is inappropriate for minors. The term “harmful to minors” as used above means any picture, image, text, graphic image file 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.

F. Cyber Bullying and Response, Social Media, and Chat Rooms. The student code of conduct contained in the student handbook and the district policy on Hazing and Bullying applies to students and their online behaviors. Students shall not use technology to harass or bully other students at any time including on the bus, at school, or during a school activity. Students who have been bullied should report the bullying to nearest supervising adult as soon as possible. The district provides a confidential means to report bullying issues at <http://www.publicschoolworks.com/SHL/bullyingMgr.asp?di=126>.

To combat cyber bullying, the district has adopted age-appropriate curriculum for all students. The district will also report the instances of bullying on the district website twice annually and send information home to parents about bullying policies and how parents can help.

## **V. Privacy**

Network and Internet access is provided as a tool for your education. The 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 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/her access to the computer network and Internet terminated and which the District may refuse to reinstate for the remainder of the student's enrollment in the 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. Furthermore, a user violates this policy if he/she 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 District may also take other disciplinary action in such circumstances.

## **VII. Warranties/Indemnification**

The District makes no warranties of any kind, either expressed 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, a user is 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) is/are agreeing to indemnify and hold the school, the District, the Data Acquisition Site that provides the computer and Internet access opportunity to the 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 District's network.

## **VIII. 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.

[Adoption date: 3/11/99] [Re-adoption date: 4/5/01] [Re-adoption date: 12/15/05] [Re-adoption date: 5/24/11]

LEGAL REFS.: U.S. Const. Art. I, Section 8

Family Educational Rights and Privacy Act; 20 USC 1232g et seq.  
Children's Internet Protection Act; (P.L. 106-554, HR 4577, 2000,  
114 Stat 2763)  
ORC 1329.54-1329.67, 3313.20, 3319.321

CROSS REFS.: AC, Nondiscrimination, ACA, Nondiscrimination on the Basis of Sex, ACAA, Sexual Harassment  
IB, Academic Freedom, IIA, Instructional Materials, IIBG, Computer-Assisted Instruction  
JFC, Student Conduct, JFCK, Use of Electronic Communications Equipment by Students