

CANTON AREA

No. 252, 352, 452, 552, 815 (5 Pages)

SCHOOL DISTRICT

TITLE: Acceptable Use of Technology

ADOPTED: May 13, 2004

No. 815 Revised 6/17/2004

(also added to 252,352,452,552)

PURPOSE

The Board supports use of the Internet and other computer networks in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration.

For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

AUTHORITY

The electronic information available to students and staff does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The district shall not be responsible for any unauthorized charges or fees resulting from the access to the Internet.

The district reserves the right to log network use and to monitor fileserver space utilization by district users, while respecting the privacy rights of both district users and outside users.

The Board establishes that network use is a privilege, not a right; inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary actions.

DELEGATION OF RESPONSIBILITY

The district shall make every effort to ensure that this resource is used responsibly by students and staff.

Administrators, teachers and staff have professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

Students and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet.

The building administrator shall have the authority to determine what is inappropriate use.

Superintendent or designee shall be responsible for implementing technology and procedures to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to:

1. Utilizing a technology protection measure that blocks, or filters Internet

access for students and adults to certain visual depictions that are obscene, child pornography, harmful to students with respect to use by students, or determined inappropriate for use by students by the Board.

2. **Maintaining and securing a usage log.**
3. **Monitoring online activities of students.**

GUIDELINES

Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system.

Students and staff are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Illegal activity.
2. Commercial or for-profit purposes.
3. Non-work or non-school related work during the school day
4. Product advertisement or political lobbying.
5. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
6. Unauthorized or illegal installation, distribution, reproduction, or use of copy righted materials.
7. **Access to obscene or pornographic material or child pornography.**
8. **Access by students to material that is harmful to students or is determined inappropriate for students in accordance with Board policy.**
9. Inappropriate language or profanity.
10. Transmission of material likely to be offensive or objectionable to recipients.
11. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
12. Impersonation of another user, anonymity, and pseudonyms.
13. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
14. Loading or using of unauthorized games, programs, files, or other electronic media.
15. Disruption of the work of other users.
16. **Destruction, modification, abuse or unauthorized access to network hardware, software and files.**
17. Quoting of personal communications in a public forum without the original author's prior consent.

SECURITY

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, the following guidelines shall be followed:

1. Students shall not reveal their passwords to other students
2. Users are not to use a computer that has been logged in under another user's name.

No. 815 INTERNET – ACCEPTABLE USE POLICY Pg. 3

4. Product advertisement or political lobbying.
5. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
6. Unauthorized or illegal installation, distribution, reproduction, or use of copy righted materials.
7. **Access to obscene or pornographic material or child pornography.**
8. **Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.**
9. Inappropriate language or profanity.
10. Transmission of material likely to be offensive or objectionable to recipients.
11. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
12. Impersonation of another user, anonymity, and pseudonyms.
13. Fraudulent copying, communications, or modifications of materials in violation of copyright laws.
14. Loading or using of unauthorized games, programs, files, or electronic media.
15. Disruption of the work of other users.
16. **Destruction, modification, abuse or unauthorized access to network hardware, software and files.**
17. Quoting of personal communications in a public forum without the original author's prior consent.

5. Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, the following shall be followed:

1. Employees and students shall not reveal their passwords to another individual.
2. Users are not to use a computer that has been logged in under another students' or employees' name.
3. Any user identified as a security risk of having a history of problems with other computer systems may be denied access to the network.

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of the network; intentional deletion or damages to files of data belonging to others; copyright violations; and thefts of services will be reported to the appropriate legal authorities for possible prosecution.

No. 815 INTERNET- ACCEPTABLE USE POLICY Pg. 4

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use.

Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

6. Copyright

The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.

7. Safety

To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc.

Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.

Internet safety measures shall effectively address the following:

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.
2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.
4. Unauthorized disclosure, use and dissemination of personal information regarding minors.
5. Restriction of minor's access to materials harmful to them.

3. Any user identified as a security risk of having a history of problems with other computer systems may be denied access to the network.
4. Faculty have read permission rights to all student files.
5. Employees maybe required to share their password with the in house technical support personnel.

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of the network; intentional deletion or damages to files of data belonging to others; copyright violations; and thefts of services will be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use.

Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

COPYRIGHT

The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.

SAFETY

To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report such immediately to a teacher or administrator. **Network users shall not reveal unauthorized information to other users on the network, including chat rooms, e-mail, Internet, etc.**

Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.

Internet safety measurers shall effectively address the following:

1. **Control of access by students to inappropriate matter on the Internet and World Wide Web.**
2. **Safety and security of students when using electronic mail, chat rooms, and other forms of direct electronic communications.**
3. **Prevention of unauthorized online access by students, including "hacking" and other unlawful activities.**
4. **Unauthorized disclosure, use, and dissemination of personal information regarding students.**
5. **Restriction of student's access to materials harmful to them.**
6. **Students are to be advised that logs of their online actions maybe released to State, Local and Federal Authorities as required by law.**
7. **All Internet activity is being monitored.**

RULES AND CODE OF ETHICS AGREEMENT
FOR NETWORK AND INTERNET USERS
Canton Area School District

Section 1: To be signed by student

I understand that Canton Area School District reserves the right to

- Log Internet use and monitor files server space utilization by users.
- Remove a user account on the network.
- Access stored materials

I understand that violations of the Rules and Code of Ethics described above will be dealt with seriously.
Violators risk:

- Losing computer privileges on a temporary or permanent basis; and/or
- Disciplinary action; and/or
- Academic sanctions; and/or
- Prosecution for violation of local, state and federal laws.

I have read the Canton Area School District Rules and Code of Ethics for network and Internet users and agree by its terms. I further understand that violation of the regulations may lead to my access privileges being revoked, school disciplinary action, academic sanctions, and/or appropriate legal action.

Student's name (please print) _____

Signature _____ Date _____

Section 2: to be signed by parents

We, parents of (please print your son/daughter's name) _____

Have read and discussed with our son/daughter the above Rules and Code of Ethics for Canton Area School District computer users. We recognize that it is impossible for the School District to restrict access to all controversial materials and we will not hold the District, its employee, or the Internet provider responsible for materials acquired on the network.

We hereby give permission for our child to have user access to the Internet and the network at his/her school. We realize that under law we may be held financially responsible for the willful, malicious, or unlawful damage of property by our child.

Parent/guardian name (please print) _____

Parent/guardian signature _____ Date _____

The Canton Area School District Web Page would like to use photographs of students involved in various academic, interscholastic athletics and co-curricular activities throughout the year. We will use those photographs if both the student and their parent/legal guardian give the district permission. No identifying information about the student (name, address, grade) will be used. This agreement will be in effect for the duration of this school year only. A new form must be completed each school year. You may terminate this agreement by contacting the school district at any time.

I give the Canton Area School District permission to use a photograph of my child on the district web page.

Signature of Parent/Guardian _____ Date _____

I give the Canton Area School District permission to use my photograph on the district web page.

Signature of Student _____ Date

COMPUTER LAB HEADPHONES

All students will be assigned to the computer lab for curriculum work two or three periods per week.

Each student will be issued a set of headphones to wear while on the computer. The headphones will be worn only by that student and will be stored in a sealed bag. The headphones will remain in the lab for computer use only.

All students must take care of their set of headphones. Any student caught vandalizing the headphones must pay for a new set (\$10.00).