Colonial School District

Section: Operations

Title: Acceptable Use Of Internet And School Computer Network

Adopted: April 21, 2005

Revised: August 19, 2010
Revised: May 16, 2013
Revised: February 26, 2015

815. Acceptable Use of Internet and School Computer Network

Purpose

The district is committed to incorporating technology into all facets of educational and administrative operations in order to:

1. Address the diverse needs of all members of the school community.
2. Prepare and empower individuals to succeed in a rapidly changing global society.
3. Facilitate and enrich learning and the instructional process.
4. Access, integrate, and manage information and resources, and enhance internal and external communication.

All use of the district's computer network and the Internet must be in support of education and research, consistent with the mission and goals of the district.

The computer network and the Internet will be used to support the district's curriculum, the educational community, projects between schools and communications and research for district students, teachers, and administrators.

Authority

The district makes no warranties of any kind, either express or implied, in connection with its provisions of access to and use of its computer networks and the Internet provided under this policy. The district 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 arising out of the use of its computer networks or the Internet under this policy.

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

The district reserves the right to log Internet use and to monitor fileserver space utilization by district users, while respecting the privacy rights of both district users and outside users. To the extent that the district maintains electronic records made private by law, regulation, order or district policy, the district will utilize its best efforts and industry standard measures to protect such records from unauthorized access or release.

47 U.S.C. Sec. 254

The Board establishes that use of the district's computer facilities is a privilege, not a right; the district reserves the right to remove a user account from the network to prevent further unauthorized or illegal activity. Additional sanctions shall apply, as appropriate.

The Board shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors.

Delegation of <u>Responsibility</u>

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

Administrators, teachers and staff have a 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 inappropriate use. Each building's administrators shall promulgate guidelines related to appropriate and inappropriate use by students in that building.

20 U.S.C. Sec. 6777
47 U.S.C. Sec. 254

The 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 minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board.
2. Maintaining and securing a usage log.
3. Monitoring online activities of minors.

20 U.S.C.
Sec. 6777
47 U.S.C.
Sec. 254

Internet filtering software or other technology-based protection systems may be disabled at the written request of a supervising teacher or school administrator for purposes of bonafide research or other legitimate educational project not dealing with materials that are specifically prohibited under law. Such requests shall be maintained in a file in the building principal's office.

Guidelines

Network accounts shall be used only by the authorized owner of the account for its authorized 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.

The use of the Internet and/or the district's computer network for illegal, inappropriate, or unethical purposes by students or employees is prohibited. Specifically:

1. Use of the network to facilitate illegal activity is prohibited.
2. Use of the network for commercial or for-profit purposes is prohibited.
3. Use of the network for nonwork or nonschool related work is prohibited.
4. Use of the network for nonschool related product advertisement or political lobbying is prohibited.
5. Malicious use of the network to develop programs that harass other users or infiltrate a computer system and/or damage the software of a computer or system is prohibited.
6. Conduct using any form of communication over the District's network or using the District's computer resources in a manner qualifying as harassment or bullying (each as defined elsewhere in District policy), or otherwise transmitting unwelcome remarks or engaging in conduct based upon sex, race or other protected characteristics which could be reasonably and objectively understood to unreasonably interfere with a student's education or employee's position within the District, or using the District's network or computer resources to send threatening statements and other similar antisocial communications. In using the district's Internet access, students are not to reveal personal information of themselves or others, such as home address, telephone, or last name.
7. Students are not to arrange face-to-face meetings with persons met online without written permission of their parents/guardians.
8. The unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials in district computers is prohibited.
9. Use of the network to access or transmit obscene or pornographic

material or child pornography is prohibited.

10. Inappropriate language or profanity is prohibited.
11. Use of the network to intentionally obtain or modify files, passwords, or data belonging to other users is prohibited.
12. It is a violation of this policy to use the district's computer networks or Internet access to gain, or attempt to gain, unauthorized access to other computers or computer systems.
13. Use of the network to misrepresent other users on the network through impersonation, anonymity, and pseudonyms is prohibited.
14. Use of the school technology or the network for fraudulent copying, communications, or modifications of materials in violation of copyright law is prohibited and will be referred to appropriate authorities.

17 U.S.C. Sec. 101 et seq

15. Loading or use of unauthorized games, programs, files, or other electronic media is prohibited.

Pol. 814

16. The network shall not be used to disrupt the work of others, and the hardware or software of other users shall not be destroyed, modified, or abused in any way.
17. Use of the network which results in any copyright violation is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.
18. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors is prohibited.
19. Quoting of personal communications in a public forum without the original author's prior consent is prohibited.

Student Code Of Ethics

Students must pledge to adhere to rules and Board policy governing the use of the district's computer facilities. These rules govern fair use, use for strictly academic purposes, privacy of information, copyright, security, tampering, mischief and attempts to disrupt computer operations.

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. 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 student's or employee's name.
3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Consequences For Inappropriate Use

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

Failure to follow the guidelines and prohibitions listed in this policy may result in the loss of the right of access to the network. Other appropriate disciplinary action may take place for students and employees.

Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations; and theft 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.

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.

47 U.S.C. Sec. 254

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. This shall include a requirement that instructional staff may not require the use of any web site or web-based service that collects personal data about its users where those users are under 13.
5. Restriction of minors' access to materials harmful to them.

Education

Education in the proper use of technology resources will be provided for both employees and students with emphasis on safe and responsible use. Education is designed to promote district standards and acceptable use of technology resources as set forth in this policy and any guidelines promulgated by the Superintendent, the Superintendent's designee, or the building principals. Education shall promote student safety in electronic communications, including the internet, appropriate online behavior, and cyber bullying awareness and response.

References:

Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.
U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq.
Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777
Internet Safety – 47 U.S.C. Sec. 254
State Board of Education Regulations – 22 PA Code Sec. 403.1