Board of Education Policy

STUDENT COMPUTER NETWORK ACCEPTABLE USE AND INTERNET SAFETY

(Terms and Conditions for Use of the Internet and Computer Networks)

The District's goal in providing Internet and computer network services to administrators, teachers, and students is to promote educational excellence by facilitating resource sharing innovations and communications.

Under appropriate supervision, students may have access to:

1. Electronic mail communication. This access may be available only through an approved faculty account. Students shall not have access to individual e-mail account. Students may not, for example, access their personal account (home-based account) through district equipment;
2. Information and news from a variety of research institutions in the fields of education, government, science and technology, social science, humanities and commercial enterprises;
3. Software used in furtherance of educational purposes and research consistent with the District's mission and goals;
4. Discussion groups, newsgroups and list servers; and
5. University library catalogs, the Library of Congress, ERIC, museums, etc.

The District has taken precautions to deny access to restricted areas of the local network. However, on a global network, it is impossible to control all materials and to completely prevent access to controversial information in written and graphic form. The District, through appropriate levels of administration and staff, shall monitor the use of the Internet/computer networks authorized by this policy. There shall be no unauthorized and/or otherwise inappropriate installation or use of hardware, software, or access to information on the internet. Any unauthorized or otherwise inappropriate use or installation of hardware, software or access to the aforementioned information, may result in the cancellation of user privileges and/or disciplinary action if deemed appropriate.

The safe, smooth operation of the network relies upon the proper conduct of the end user, who must adhere to strict guidelines. In general, this requires efficient, ethical, and legal utilization of the network resources. If a District user violates any of these provisions, his or her account may be terminated and future access may be denied. The signature of the user on the required Acknowledgement of Responsibilities form is legally binding and indicates that the party who executed same has read the terms and conditions carefully and understands their significance.

1. Acceptable Use: The use of a network account must be in support of education and research and consistent with the educational objectives of the District. Use of another organization's network or computing resources must comply with the rules appropriate for that network.

2. Prohibited Activities and Uses: The following is a non-exclusive list of prohibited activity concerning use of the District computer network. Violation of any of the following prohibitions may result in discipline, including suspension or revocation of a user's access to the network.
    a. Unauthorized use of the network for commercial and/or non-District business activity, including advertising.

b. Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the District computer network.

c. Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material.

d. Using the network to receive, transmit or make available to others messages that are threatening, obscene, racist, sexist, abusive, harassing, or otherwise inconsistent with the District's Code of Conduct.

e. Using another user's account or password.

f. Unauthorized interference with the ability of other system users to use the Internet or network.

g. Forging or attempting to forge e-mail messages.

h. Engaging in vandalism, as defined below.

i. Unauthorized disclosure of the personal address, telephone number or other personally identifiable student information of oneself or another person

j. Intentionally disrupting network traffic or crashing the network and connected systems.

k. Unauthorized installation of personal software or using personal disks on the District's computers and/or network without the permission of the appropriate District official or employee.

l. Using District computing resources for commercial or financial gain, or fraud.

m. Stealing data, equipment or intellectual property.

n. Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, electronic mail (email) accounts, or vandalize the data of another user.

o. Using the Internet/Computer Network while access privileges are suspended or revoked.

p. Using abusive or offensive language, including the use of vulgarities, swearing, and name-calling.

q. Any unauthorized purchase of items via the Internet or subscribing to commercial services.

r. Bypassing or hindering security measures.

s. Using the Internet in any illegal manner.

t. Unauthorized use of encryption software.

u. Accessing the Internet using a non-District account.

v. Sharing of network user passwords or u sing another user's account or password.

3. Privileges: The use of the Internet/Computer Network is a privilege, not a right, and inappropriate use may result in suspension or revocation of that privilege by the Superintendent or his/her designee. Students using the District's computer network should not expect, nor does the District guarantee privacy for electronic mail (email), files, or any use of the District's computer network. District reserves the right to access and view any material stored on District equipment or any material used in conjunction with the District's computer network. Message or other electronic data relating to or in support of illegal activities may be reported to the authorities or the Superintendent or his/her designee. Any problems and/or questions must be directed to the Superintendent or such designee. The Superintendent, administration, faculty and staff of the District may deny, revoke, or suspend specific user accounts at their discretion for any misuse or violation of this policy. Individuals have the full responsibility for the use of their accounts. Any such sharing of passwords or the use of accounts is prohibited. All recipients of accounts must participate in training pertaining to the proper use of the network. All network users will be issued a login name and password. Passwords must be changed periodically. Account users are responsible for maintaining a current password. The Superintendent or designee will conduct a yearly review of all accounts to determine adherence to this policy.

4. Netiquette: Individuals are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:
    a. Be polite. Do not be abusive in your messages to others;
    b. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language;
    c. Do not reveal your personal address, phone number, and credit card number or those of students or colleagues;
    d. Note that electronic mail (e-mail) and data files are not guaranteed to be private. In fact, users have no reasonable expectation of privacy in connection with e-mail or other data and information they create, send and/or receive through District computer equipment, systems, or networks. In addition, District personnel, consultants and/or professionals who operate and/or maintain the systems DO have access to all e-mail and other data and information and will monitor same periodically and/or at the direction of District Administration. Messages or other electronic data relating to or in support of illegal or inappropriate activities may be reported to law enforcement authorities or the Superintendent or his/her designee and may result in disciplinary action being taken against violators;
    e. Do not use the network in such a way that will disrupt its use by others;
    f. All communications and information accessible via the network must be assumed to be the property of the provider;
    g. Use of the computer equipment systems or network and data acquired must be in strict compliance with the law; and
    h.

i. Follow the directions of all staff and faculty members regarding computer usage and lab etiquette. Failure to do so will be considered insubordination and will be consequenced as such. Disciplinary action may include, but will not be limited to:

Minor offense: Suspension of computer privileges, conference with student, and/or detention one – to – three days; and

Major offense: Suspension or cancellation of computer privileges, detention, up to five days suspension and/or parental/guardian conference.

5. Disclaimer: The District makes no warranties of any kind, whether expressed or implied, for the service access or information it is providing pursuant to this policy. The District will not be responsible for any damage suffered. This includes loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by the District's negligence or error or omissions. Use of any information obtained from the District's computer network or internet is at the user's own risk. Any violation of State, Federal or local laws, ordinances, rules or regulations, and any attended penalties shall be the sole responsibility of the user. The District specifically denies and assumes no responsibility for the accuracy, ~~or~~ quality, availability, reliability or nature of the information and/or service obtained through the District's Internet. It is the responsibility of each user to verify the integrity and authenticity of the information that is used.

6. Commercial Services: Commercial services are available on the Internet. If a user chooses to access these services, the user is liable for any costs that are incurred as a result of the user's unauthorized use of commercial services on the Internet.

7. Security Issues: If any user identifies a security problem on the Internet/Computer Network, they must notify the Superintendent or designee. Under no circumstances should the user show such security problem to anyone other than to the Superintendent of his/her designee. Attempts to login to the Internet/Computer Network, as a system administrator will, at the very least, result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the Internet/Computer Network.

4. Vandalism: Vandalism will result in the cancellation of privileges, and consequences will be applied as described in the District's policy on Vandalism. Vandalism includes any malicious attempt to harm or destroy District equipment, software or data, or that of another user, any agencies, or other networks that are connected to the Internet. This includes, but is not limited to placing, uploading, and/or creating a computer virus~~es~~ on the network. In the case of vandalism to District equipment, the user will be financially responsible to reimburse the District for repairs and/or replacement of such equipment and such conduct may result in discipline and/or be reported to the authorities.

8. Student Education: The school District will educate students on bullying, cyberbullying, harassment, internet safety, appropriate online behavior including interacting with other individuals on social networking websites, and in chat rooms and cyberbullying awareness and response through age-appropriate instruction provided in course curriculum, student assemblies or classroom instruction.

9. Internet Safety: The Board of Education directs the Superintendent to procure and utilize technology that blocks and/or filters Internet access to websites or visual depictions that display obscenity, child pornography, or any other content that is otherwise harmful to minors. These measures may only be disabled or relaxed if access to the restricted content is necessary to meet a legitimate educational or District purpose.

Adopted:	04/18/1996		
Reviewed:	01/16/2002	06/23/2010	12/10/14
Revised:	01/16/2002	07/06/2010	01/28/15