EMPLOYEE COMPUTER NETWORK ACCEPTABLE USE & INTERNET SAFETY

The District's goal in providing Internet and computer network services to staff is to promote educational excellence by facilitating resource sharing innovations and communications:

Under appropriate supervision, staff may have access to:

1. Electronic mail communication. This access may be available only through an approved staff account. Staff shall not have access to personal e-mail accounts when using 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 of all types;
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 its 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. Each user will be required to sign an Acknowledgement of Responsibilities form, indicating that the party who executed same has read the terms and conditions carefully and understands their obligation to comply with those terms and conditions, including the potential consequences for failing to do so.

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's 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 or 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's 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 or harassing to others.
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 personal address, telephone number or other personally identifiable information.
j. Intentionally disrupting network traffic or crashing the network and connected systems.
k. Unauthorized installation of personal software or using personal flash drives 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, or vandalize the data of another user.
o. Using the network while access privileges are suspended or revoked.
p. Using abusive or offensive language, including the use of vulgarities, swearing, and/or name-calling.
q. Unauthorized purchase 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.

3. Privileges: The use of the Internet/Computer Network is a privilege, not a right, and inappropriate use may result in cancellation of such account(s) by the Superintendent or his/her designee. Note that electronic mail (e-mail) and data files are not guaranteed to be private. The "end-users" who operate the systems do not have access to all e-mail and data. Only

authorized personnel in the District has access to all e-mail and data. Message(s) or other electronic data relating to or in support of illegal activities will be reported to the authorities, the Superintendent or his/her designee. Any problems and/or questions with regard to suspicious emails, data, or other District technology resources must be directed to the Superintendent or such designee. The Superintendent or designee of the District may deny, revoke, or suspend specific user accounts at their discretion for any misuse or violation of this policy. Individuals are fully responsible for the use of their accounts, and, under no circumstance, may anyone share their account or password with any other person. Any such sharing of passwords or the use of accounts is prohibited. As deemed appropriate, all recipients of accounts must participate in training pertaining to the proper use of the network. Account users are responsible for maintenance of their accounts. The Superintendent or designee will conduct a yearly review of all accounts to determine adherence to this policy.

Netiquette: Individuals are expected to abide by the generally accepted rules of network etiquette, which 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, credit card number or those of students, colleagues, or any other person;
d. Note that electronic mail (e-mail) and data files are not guaranteed to be private. 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, only authorized 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 system and the data acquired must be in strict compliance with the law; and
h. Follow the directions of the administrative staff regarding computer usage and lab etiquette.

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 shall have no responsibility for use of the system by employees who abuse the system and/or violate this Policy, Regulation, and/or the law. Use of any information obtained is at the user's 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 responsibility for the accuracy or quality of information obtained through Internet services. 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 may be incurred. As noted, commercial activities are not supported by the District.

7. Security Issues: If any user identifies a security problem on the Internet/Computer Network, they must immediately notify the Superintendent or his/her designee. Attempts to login to the Internet/Computer Network, as a system administrator may, at the very least, result in cancellation of user's account(s). 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.

8. Vandalism: Vandalism will result in the cancellation of account access and use, 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 or creating a computer virus 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 appropriate law enforcement authorities.

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.

10. Personal Devices: The Board authorizes use of employee personal devices to access the District's computer network if the employee complies with the District's registration process, as well as the provisions of this policy. Failure to register or abide by this policy and regulation will result in revocation of access and possible disciplinary action in accordance with the law and/or the Code of Conduct.

Adopted:	10/24/2007					
Reviewed:	11/28/2007	06/23/2010	12/10/2014	03/29/2017	04/17/2019	03/29/2023
Revised:	11/28/2007	07/06/2010	01/28/2015	04/26/2017	05/29/2019	04/26/2023