Book	Policy Manual
Section	4000- Instruction
Title	Acceptable Use of School District Computers and Computer Networks
Number	4526
Status	Active
Legal	Reviewed by Counsel December 4, 2014
Adopted	January 11, 2018
Last Revised	December 13, 2017
Last Reviewed	December 13, 2017

The Board of Education is committed to optimizing student learning and teaching. The Board of Education considers student access to a computer network, including the Internet, to be a powerful and valuable educational and research tool, and encourages the use of computers and computer related technology in School District classrooms for the purpose of advancing and promoting learning and teaching.

The computer network can provide a forum for learning various software applications and through online databases, bulletin boards and electronic mail, can significantly enhance educational experiences and provide statewide, national and global communication opportunities for staff and students.

The Board of Education authorizes use of personal electronic device(s) to access the School District's computer network for educational purposes. Individuals connecting to the School District network are required to comply with the School District's Internet Safety Policy, as well as the provisions of this policy. Failure to abide by this policy will result in revocation of access and possibly disciplinary action in accordance with the Code of Conduct.

The Superintendent of Schools shall be responsible for designating an individual(s) to oversee the use of School District computer and networking resources. Said individual(s) will prepare in-service programs for the training and development of School District staff in computer skills, and for the incorporation of computer use in appropriate subject areas.

The Superintendent of Schools, working in conjunction with the designated purchasing agent for the School District, the individual(s) assigned to oversee the use of School District computer and networking resources and the instructional materials planning committee, will be responsible for the purchase and distribution of computer software and hardware throughout the School District’s schools. They shall prepare and submit for the Board of Education's approval a comprehensive multiyear technology plan which shall be revised as necessary to reflect changing technology and/or School District needs.

All users of the School District's computer network and equipment shall comply with this policy. All users of the School District's computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility. The School District reserves the right to control access to the Internet for all users of its computers and network. The School District may either allow or prohibit certain kinds of online activity, or access to specific websites.

The following rules and regulations govern the use of the School District's computer network system and access to the Internet.

1. Administration

a. The Director of Technology and Information Systems and the Director of Information Management shall:
   - oversee the School District's computer network;
   - monitor and examine all network activities, as appropriate, to ensure proper use of the system;
   - be responsible for disseminating and interpreting Board of Education and School District policy and regulations governing use of the School District's network at the building level with all network users;
   - provide employee training for proper use of the network and will ensure that staff supervising students using the School District's network provide similar training to their students, including providing copies of Board of Education and School District policy and regulations governing use of the School District's network; and

- ensure that all files, data, and/or software loaded onto the computer network have been scanned for computer viruses.

b. All student agreements to abide by Board of Education and School District policy and regulations and parental consent forms shall be kept on file in the school building that the student attends.

2. Acceptable Use and Conduct

a. All network users will be issued a login name and password. Passwords must be changed periodically.

b. Only those network users with written permission from the Superintendent of Schools or his/her designee may access the School District's internal network from off site (e.g., from home).

c. All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive or sexual language or images, vulgarities and swear words are not appropriate.

d. Network users identifying a security problem on the School District's network must notify the appropriate teacher, administrator or Director of Technology. Under no circumstance should the user demonstrate the problem to anyone other than to the School District official or employee being notified.

e. Any network user identified as a security risk or having a history of violations of the School District computer use guidelines may be denied access to the School District's network.

f. All users must act in ways that do not invade the privacy of others, and/or comply with all legal restrictions regarding the use of electronic data.

g. All users must maintain the confidentiality of student information in compliance with federal and state law. Disclosing and/or gossiping (including but not limited to via e-mail, voice mail, Internet instant messaging, chat rooms or on Web pages) about confidential or proprietary information related to the School District is prohibited.

h. All users must refrain from acts that waste School District technology resources or prevent others from using them. Users will not access, modify or delete others' files or system settings without express permission. Tampering of any kind is strictly forbidden. Deliberate attempts to tamper with, circumvent filtering or access, or degrade the performance of a School District computer system, telephone system or network or to deprive authorized users of access to or use of such resources are prohibited.

i. Users are responsible for both the content and possible effects of their messages on the network. Prohibited activity includes, but is not limited to, creating or propagating viruses, material in any form (text, sound, pictures or video) that reflects adversely on the School District, "chain letters" (which proffer incentives to relay them to others), inappropriate messages (including discriminatory, bullying or harassing material), and billable services.

j. Official email communications must be professional, ethical and meet the standards of other School District publications bearing in mind that the writer is acting as a representative of the School District and in furtherance of the School District's educational mission.

k. Users are prohibited from using personal links and addresses such as blogs, YouTube videos, etc. in School District email unless used in the furtherance of business of the School District or as part of the curriculum of the School District. The signature portion of the user's email may not include external links or graphics that are unrelated to the content of the email.

l. Altering electronic communications to hide the identity of the sender or impersonate another person is illegal, considered forgery and is prohibited.

m. Users will abide by all copyright, trademarks, patent and other laws governing intellectual property. No software may be installed, copied or used on School District equipment except as permitted by law and approved by the District Director of Technology. All software license provisions must be strictly adhered to.

n. Since the installation of applications other than School District-owned and School District-tested programs could damage the School District's computer systems or interfere with others' use, software downloaded from the Internet or obtained elsewhere must be approved by the District Director of Technology or his/her designee. Software may not be installed onto any School District-owned or School District-leased computer by an individual other that the District Director of Technology or his/her designee.

o. Use of voice mailboxes for commercial purposes or advertising is not permitted. Use of security codes is required in order to guarantee privacy for mailbox users. Override permission codes are held by Operations and Maintenance.

3. Account Access to Network, E-Mail Accounts and Computer Services

a. All student users of the network or computer services may access resources according to his/her assigned rights, with appropriate authorization and parent consent. Approved class work shall have priority over other uses. No single user is allowed to monopolize a computer, unless specifically assigned for special needs.

b. All use of the network or other on-line servers must be in support of education and research consistent with the goals of the School District. The term "education" includes use of the system for classroom, professional or career development activities.

c. Users are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to access their accounts. Users will be held responsible for any policy violations that are traced to their accounts. Under no conditions shall a user provide his/her password to another person.

d. Users may be required to remove files if total system storage space becomes low.

e. Electronic files stored on the school computers may be reviewed by school personnel at any time.

f. The use of "chat rooms" for purposes other than education is strictly forbidden.

g. Students will be allowed Internet access for instructional purposes.

4. System Security

a. Software shall be installed by authorized School District computer administration personnel only.

b. The permission of the Director of Technology and Information Systems or the Director of Information Management is necessary in order to download or install software.

c. Permission of the Director of Technology and Information Systems or the Director of Information Management is required for relocation, removal or adjustment of any hardware and/or peripheral device

d. Food and/or drink shall not be placed in the immediate area where computers are located.

e. Use of personal equipment (expressly permitted in this policy) including, but not limited to printers, scanners, wireless access points (WAP), and switches, is forbidden without special permission from the Director of Technology or the Director of Information Management.

5. Plagiarism and Copyright Infringement

a. Any software that is protected under copyright laws will not be loaded onto or transmitted via the network or other on-line servers without the prior written consent of the copyright holder.

b. Users will honor all copyright rules and not plagiarize or use copyrighted information without permission. Plagiarism is the use of writings or ideas of others and presenting them as if they were the creation of the presenter.

c. The School District will receive written permission from parents and/or guardians prior to publishing any student's work on the Internet or School District web pages.

6. Prohibited Activities

a. Users will not knowingly or recklessly post false or defamatory information about a person or organization.

b. Attempts to log on through another person's account or to access another person's files are illegal and this conduct shall not be engaged in, except that the School District's administrators shall have the right to log on through another person's account and access another person's files for network security reasons or other reasons within their discretion.

c. Any use of the Internet or network for profit is prohibited.

d. Any use of the Internet or network software for a purpose or effect that is deemed by the supervising staff member and/or school administration to be dangerous, objectionable, pornographic, distracting to education, or otherwise offensive in nature is prohibited.

e. Users will not post chain letters or send messages to large numbers of people.

f. Electronic hate mail, harassment, discriminatory remarks, inappropriate language and other illegal and/or antisocial behaviors are prohibited.

g. Users of the network shall only use their assigned passwords and not seek to misrepresent themselves as other users.

h. Users may not use the School District system to engage in any illegal act, such as arranging for a drug sale, purchasing alcohol, promoting violent or terrorist activity, engaging in criminal activity, threatening the safety of a person, etc.

i. Unauthorized exploration of the Network Operating System or unauthorized changes to any installed software is strictly prohibited.

j. Student Internet access may be restricted depending on the grade level. All users will be prohibited from accessing social networking sites; playing online games; using personal email services; and watching videos online (unless authorized for a school purpose).

7. Personal Use

a. Users may not use the School District system for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use.
b. Users may not use the system for political lobbying in support of or opposition to individual candidates or political parties.
c. Users may not post personal information about themselves or others, such as their last name, home address, work address, phone number, school name or address.
d. Users will not transmit pictures of themselves or others.

8. Personal Safety Restrictions for Students

a. Users will, as soon as practical, disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.
b. Users will not meet with strangers they have met on line.

9. **Confidentiality and Privacy Rights**

Individuals must take all reasonable precautions to prevent unauthorized access to accounts or data by others, both inside and outside the School District. Individuals will not leave any devices unattended with confidential information visible. All devices are required to be locked down when an individual steps away from the device, and settings enabled to freeze and lock after a set period of inactivity.
Data files and electronic storage areas shall remain School District property, subject to School District control and inspection. The District Director of Technology may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy.Individuals using the School District's computer network should not expect, nor does the School District guarantee, privacy for electronic mail (e-mail) or any use of the School District's computer network. The School District reserves the right to access and view any material stored on School District equipment or any material used in conjunction with the School District's computer network.
Individuals using the School District's computer network should not expect, nor does the School District guarantee, privacy for electronic mail (e-mail) or any use of the School District's computer network. The School District reserves the right to access and view any material stored on School District equipment or any material used in conjunction with the School District's computer network.

10. Security

a. Each user is responsible for the security and integrity of information stored on his or her computer or voice mail system. Computer accounts, passwords, security codes and other types of authorization are assigned to individual users and must not be shared with or used by others. The School District, at its sole discretion, reserves the right to bypass such passwords and to access, view or monitor its systems and all of their contents. By accessing the School District's computer system, the user has consented to the School District's right to access any and all information thereon.
b. Removing or relocating School District-owned technology resources require prior authorization from the District Director of Technology.
c. Users may not attempt to circumvent or subvert the security provisions of any other system. No one may attach a server to or provide server services on the School District network.

11. Vandalism

a. Any act of vandalism is strictly prohibited. Vandalism is the malicious attempt to destroy or harm data or equipment.
b. Uploading, creating or spreading computer viruses is considered to be an act of vandalism.

c. Unauthorized tampering or mechanical alternation, including software configurations is considered to be vandalism.

12. Access to Inappropriate Material

a. Users will not utilize the School District system to access material that is profane or obscene, that advocates illegal acts, or that advocates violence or discrimination towards other people. For students, a special exception to certain sensitive materials for projects may be made for literature if the purpose of such access is to conduct research and the access is approved by the teacher or administrator.

b. The user should, as soon as practical, disclose any inadvertent access in a manner specified by their school. This will protect them against an allegation that they have intentionally violated this Acceptable Use Policy.

13. Inappropriate Materials

1. The School District prohibits any individual, including faculty, staff and students, from developing, maintaining, and transmitting pornography in any form at school, including, but not limited to, magazines, posters, videos, electronic files or other electronic materials.

2. Accessing the School District's network or equipment to create, access, download, edit, view, store, send or print materials that are illegal, offensive, harassing, intimidating, discriminatory, sexually explicit or graphic, pornographic, obscene, or which constitute sexting or cyberbullying or are otherwise inconsistent with the values and general standards for community behavior of the School District is prohibited. The School District will respond to complaints of harassing or discriminatory use of its technology resources in accordance with its Anti-Harassment and Anti-Discrimination Policy.

14. Use of Personal Electronic Devices

Personal electronic devices include, but are not limited to, personal laptops, smart phones, portable storage media, all recording devices, all Internet connected devices and handheld devices such as iPods and iPads. Students may use their own devices to access the Internet for educational purposes. The District reserves the right to monitor, inspect, limit use of and/or confiscate personal devices when administration has reasonable suspicion that a violation of school policy has occurred.

The School District maintains a “public” wireless network, a “private” wireless network and a “hard wired” network. The “hard wired” and “private” wireless networks are limited only to district-owned and managed devices. Any attempt to connect a personally owned device to either of these networks will be considered a violation of this policy. The “public” wireless network is the sole network that students and faculty may connect to using their own devices. The School District reserves the right to alter or disable access to the “public” wireless network as it deems necessary without prior notification.

Personal electronic devices that have the ability to offer wireless access to other devices must not be used to provide that functionality to others in any School District building. The ability to connect personal devices to the School District wireless network is a privilege and not a right. When personal electronic devices are used in School District facilities or on the School District wireless network, the School District reserves the right to:

a. make determinations on whether specific uses of the personally owned wireless devices are consistent with this policy;

b. log network use and monitor storage disk space utilized by such users; and

c. remove or restrict the user’s access to the network and suspend the right to use the personal electronic device in School District facilities at any time if it is determined that the user is engaged in unauthorized activity or in violation of Board of Education policy.

d. Personal electronic devices connected to the School District’s computer system or wireless network must have updated and secure operating systems and proper forms of anti-virus and anti-malware protection. Individuals must not make any attempt to connect devices that are not properly secured.

e. The cost to acquire all personal electronic devices is the responsibility of the individual. Services that include a financial cost to the School District, such as phone options or other "apps" are not allowed. The School District does not agree to pay such charges and individual who desire these options must assume all costs incurred for such charges.

f. Personal electronic devices are not covered by the School District's insurance if lost, stolen or damaged. Loss or damage to any personal electronic device is solely the responsibility of the individual. If lost or stolen, the loss should be reported immediately to District’s Director of Technology so that appropriate action can be taken to minimize any possible risk to the School District’s computer system and the School District.

g. Individuals using personal electronic devices are responsible for their maintenance of personal electronic devices, including maintenance to conform to School District standards. Individuals using personal electronic devices also assume all responsibility for problem resolution, as well as the use, maintenance and cost of functional, up-to-date anti-virus and anti-malware software and any other protections deemed necessary by the District Director of Technology or his/her designee.

h. Individuals using personal electronic devices must also meet any expectations of continuity in formatting of files, etc. when making changes to documents for School District related purposes (i.e., do not change the format of a file so that the original file is unusable on School District-owned hardware/software).

i. All personal electronic devices used on the School District's computer system or wireless network are subject to review by the District Director of Technology, or individuals/entities designated by the Superintendent of Schools, if there is reason to suspect that the personal electronic device is causing a problem to the School District's computer system and/or network.

j. The use of personal electronic devices in the course of an individual's School District related responsibilities may result in the equipment and/or certain data maintained on it being subject to review, production and/or disclosure (i.e., in response to a FOIL request, discovery demand or subpoena) and are required to submit any such information or equipment, when requested.

k. Individuals using a mobile device, personal or District-owned, are responsible for ensuring that all security protocols normally used in the management of School District data on conventional storage infrastructure are also applied on that mobile device. All School District-defined processes for storing, accessing and backing up data must be used on any device used to access the School District's computer system.

In addition, when individuals choose to use their own personal electronic devices to perform job-related functions, the following will apply:

a. The School District may choose to maintain a list of approved mobile devices and related software applications and utilities. The School District reserves the right to deny any individual permission to utilize a personal electronic device within the boundaries of the district. The Superintendent of Schools or his/her designee reserves the right to make these decisions as necessary.

b. Personal electronic devices connected to the School District's computer system or wireless network must have updated and secure operating systems and proper forms of anti-virus and anti-malware protection. Individuals must not make any attempt to connect devices that are not properly secured.

c. The cost to acquire all personal electronic devices is the responsibility of the individual. Services that include a financial cost to the School District, such as phone options or other "apps" are not allowed. The School District does not agree to pay such charges and individuals who desire these options must assume all costs incurred for such charges.

d. Personal electronic devices are not covered by the School District's insurance if lost, stolen or damaged. Loss or damage to any personal electronic device is solely the responsibility of the individual. If lost or stolen, the loss should be reported immediately to District's Director of Technology so that appropriate action can be taken to minimize any possible risk to the School District's computer system and the School District.

e. Individuals shall remain responsible for their maintenance of personal electronic devices, including maintenance to conform to School District standards. Individuals also assume all responsibility for problem resolution, as well as the use, maintenance and cost of functional, up-to-date anti-virus and anti-malware software and any other protections deemed necessary by the District Director of Technology or his/her designee.

f. Individuals must also meet any expectations of continuity in formatting of files, etc. when making changes to documents for work/school purposes (i.e., do not change the format of a file so that the original file is unusable on School District-owned hardware/software).

g. All personal electronic devices used on the School District's computer system or wireless network are subject to review by the District Director of Technology, or individuals/entities designated by the Superintendent of Schools, if there is reason to suspect that the personal electronic device is causing a problem to the School District's computer system and/or network.

h. The use of personal electronic devices in the course of a staff member's professional responsibilities may result in the equipment and/or certain data maintained on it being subject to review, production and/or disclosure (i.e., in response to a FOIL request, discovery demand or subpoena). Staff members are required to submit any such information or equipment, when requested.

i. Individuals using a mobile device, personal or District-owned, are responsible for ensuring that all security protocols normally used in the management of School District data on conventional storage infrastructure are also applied

on that mobile device. All School District-defined processes for storing, accessing and backing up data must be used on any device used to access the School District's computer system.

Further, the School District will not be liable for the loss, damage, theft, or misuse of any personal electronic device(s) brought to school. The School District will bear no responsibility nor provide technical support, troubleshooting, or repair of electronic devices owned by anyone other than the School District. Students and staff are responsible for understanding and inquiring about the use of technology prior to engaging in such use.

15. Implementation

Implementation of the acceptable use policy will be the responsibility of the school administration and/or the instructors. Any appeal may be brought to the Superintendent of Schools, whose decision will be final.

16. School District Limitation of Liability

The School District does not warrant in any manner, express or implied, that the functions or the services provided by or through the School District system will be error-free or without defect. The School District shall not bear any liability for any damage suffered by users including, but not limited to, loss of data or interruption of service. Similarly, the School District shall not bear any liability for financial obligations that arise out of the unauthorized or illegal use of the system. Users of the School District's computer network and the Internet use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided. Further, even though the School District may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the Board of Education and School District policy and regulations.

Students using the School District's computer network should not expect, nor does the School District guarantee, privacy for electronic mail (e-mail) or any use of the School District's computer network. The School District reserves the right to access and view any material stored on School District equipment or any material used in conjunction with the School District's computer network.

17. No Privacy Guarantee

Students using the School District's computer network should not expect, nor does the School District guarantee, privacy for electronic mail (e-mail) or any use of the School District's computer network. The School District reserves the right to access and view any material stored on School District equipment or any material used in conjunction with the School District's computer network.

18. Sanctions

a. There are risks involved with using the Internet. To protect personal safety, Internet users should not give out personal information to others on website, chat rooms or other systems. The School District cannot guarantee that users will not encounter text, pictures or references that are objectionable. Responsible attitudes and appropriate behavior are essential in using this resource. As with e-mail, information that a user places on the Internet is akin to sending a postcard rather than a sealed letter. Its contents may be accessed by system administrators in the School District and elsewhere.

b. Users must be aware that some material circulating on the Internet is illegally distributed. Users must never use the School District's system to download illegally distributed material.

c. Users are cautioned not to open e-mail attachments or download any files from unknown sources in order to avoid damaging the School District computer system. Anything questionable should be reported immediately to the District Director of Technology.

d. With permission, students, faculty and staff may create or modify web pages on the School District web servers which comply in all respects with this policy.

Use of the School District's computer network is a privilege, not a right. Persons in violation of this policy are subject to a full range of sanctions, including, but not limited to, the loss of computer, telephone or network access privileges, disciplinary action, monetary damages and dismissal/termination from the School District. Some violations may constitute criminal offenses as defined by local, state and federal laws, and the School District may initiate or assist in the prosecution of any such violations to the full extent of the law.

All members of the School District community are expected to assist in the enforcement of this policy. Any suspected violation of this policy should be reported immediately to the Director of Technology and the Superintendent of Schools. Anyone receiving a threatening message should record/save the message and report the incident to the Principal. The Director of Technology will attempt to trace the message and report the results to the Principal and the Superintendent of Schools.

Cross-ref:

0115 Dignity for All Students Act
4526.1 Internet Safety
5300 Code of Conduct
8630 Computer Resources and Data Management
8635 Information Security Breach and Notification

Ref:

Reviewed by Counsel: December 13, 2017