District Policy

ACCEPTABLE USE OF COMPUTER NETWORKS/COMPUTERS AND RESOURCES

Overview

Access to information is fundamental to citizenship and the foundation for further educational attainment. The Board generally supports access by staff and students to educational technology that allows rich information resources along with the development of appropriate skills to analyze and evaluate such resources. The goal in providing educational technology to teachers, staff and ultimately students, is to promote educational excellence in Springfield Public Schools by facilitating resource sharing, innovation and communication. Any use of this educational technology and/or electronic communication that substantially disrupts or interferes with the orderly operation of the school or the rights of other students will not be tolerated in or outside of the school facilities or school day.

Internet Safety Protection

As a condition for receipt of certain Federal funding, the school district shall be in compliance with the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and has installed technology protection measures for all computers in the school district, including computers in media centers/libraries. The technology protection must block and/or filter material and visual depictions that are obscene as defined in Section 1460 of Title 18, United States Code; child pornography, as defined in Section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, graphic image file or other material or visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

This Policy also establishes Internet safety policy and procedures in the school district as required in the Neighborhood Children's Internet Protection Act. Policy 2361 addresses access by minors to inappropriate matter on the Internet and World Wide Web; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; unauthorized access, including "hacking" and other unlawful activities by minors online; unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors.

Notwithstanding blocking and/or filtering the material and visual depictions prohibited in the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act, the Board shall determine other Internet material that is inappropriate for minors.

In accordance with the provisions of the Children's Internet Protection Act, the Superintendent or designee will develop and ensure education is provided to every student regarding appropriate online behavior, including students interacting with other individuals on social networking sites and/or chat rooms, and cyberbullying awareness and response.

The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly Board meeting or during a designated special Board meeting to address and receive public community input on the Internet safety policy - Policy and Regulation 2361. Any changes in Policy and Regulation 2361 since the previous year's annual public hearing will also be discussed at a meeting following the annual public hearing.

The school district will certify on an annual basis, that the schools, including media centers/libraries in the school district, are in compliance with the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act and the school district enforces the requirements of these Acts and this Policy.

The Internet, for example, is an electronic communications network that provides vast, diverse and unique resources. To support the proper delivery of information via the Internet, the district has in place filtering software. Filtering software, however, is not 100% effective; while filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. It is the user's responsibility not to initiate access to materials that are inconsistent with the goals, objectives and policies of the educational mission of the district. The Board believes that the benefits to staff and students from access in the form of information resources and opportunities for collaboration exceed the disadvantages.

Internet access is coordinated through a complex association of government agencies, and regional and State networks. Recognizing that the Internet is neither a regulated nor a policed entity, the Board requests that students and staff agree to use this resource of information as an aid in the learning according to the guidelines set forth. Therefore, the smooth operation of this resource relies upon the proper conduct of the end users who must adhere to these strict guidelines. These guidelines are provided so that users are aware of the responsibilities they are about to acquire. In general, this requires efficient, ethical and legal utilization of the equipment, computers, software, and network resources.

Terms and Conditions

The use of equipment, computers, network resources and the Internet is a privilege, not a right, and inappropriate use will minimally result in the suspension and/or cancellation of those privileges. No reasonable expectation of continued use or access shall exist. The administration, faculty and staff of the Springfield Public Schools may deny, revoke or suspend specific user accounts/access. Violation of the terms of the policy may also result in more severe penalties as deemed necessary.

1. The use of an account and/or access must be consistent with the educational objectives of the Springfield Public Schools.

2. To transmit or knowingly receive any materials in violation of any United States, New Jersey, or Springfield Public Schools regulation or law is prohibited. This includes, but is not limited to, the following: copyrighted material, threatening, harassing, pornographic, obscene, or profane material, materials related to the illegal use or manufacture of restricted substances, defamatory or discriminatory material, or material protected by trade secret. Any use of this educational technology and/or electronic communication that substantially disrupts or interferes with the orderly operation of the school or the rights of other students will not be tolerated in or outside of the school facilities or school day. It may not be used to harass, intimidate or bully any person or persons. Any violation of law through the use of this technology may be dealt with through disciplinary action and may result in the suspension and/or cancelation of privileges.

3. Commercial activities, product advertising, political lobbying and extensive personal use, including spamming, are prohibited.

4. Network Etiquette - All computer users 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, material or images.

   c. Do not reveal the full name, phone number, or home address, or those of other persons when using the Internet.

   d. Note that electronic mail (email) and other computer use or storage is not guaranteed to be private or confidential. Network or other computer use or storage areas are and will be treated as school property. Computers, files and communications may be accessed and reviewed by district personnel and may be accessed by other computer users.

   e. Do not use computers or the network in such a way that would disrupt the use by other people. Talk, Write, and Chat commands may be intrusive and should only be used after receiving permission from a teacher. Chain letters and Internet relay chat are misuses of the system.

   f. Permission of the supervising staff member must be obtained before downloading large files.

   g. Disk space is limited. Remove outdated or unneeded files promptly.

   h. Gaining access to network resources with another person's account or a fictitious name is illegal.

5. Installation of software on any of the district's computer system is not allowed without approval of the Technology Department.

6. Anyone found guilty of vandalism will lose Internet privileges and may be subject to criminal prosecution. Vandalism is defined as any malicious attempt to harm or destroy data or hardware on this system or any other system.

7. Respect the integrity of the computing system. Do not intentionally develop or activate programs that harass other users, infiltrate a computer system or alter the software components of a computer or system. This includes but is not limited to revealing, or attempting to learn or use other users' passwords, spreading viruses, attempting to "hack" into restricted systems or attempting to use administrative commands.

8. Only public domain files in which the author has given expressed written consent for online distribution may be uploaded to the system. Students and teachers may download copyrighted material only for their own use following the fair use provisions in the U.S copyright law.

9. Security of any computer system is essential. Access to electronic resources is intended for the exclusive use of authorized individuals. If you feel you can identify a security problem on the Internet, you must notify a system administrator. Do not demonstrate the problem to other users. Do not use another user's account or share your account. Doing so will result in the loss of privileges for both parties.

10. Any problems that arise from the use of an account are the liability or responsibility of the account holder or user. All account holders or users hereby release Springfield Public Schools from any and all claims or damages of any nature arising from the access, use, or inability to access or use computers or the network system and by obtaining an account or use of the computers or network system agree to such and agree to indemnify and hold Springfield Public Schools harmless from same. Springfield Public School District makes no warranties of any kind for the information or the service it is providing.

11. Any student, staff or community member who seeks to use the technological resource of the district, must sign an Acceptable Use Policy Agreement. In addition, all students must have a signed parent/guardian consent form.

12. Education will be provided about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

13. Electronic devices provided by the district are equipped with recording capabilities and may record or collect information on your activity or your use of the device. Springfield Public Schools shall not use any of the recording capabilities in a manner that would violate your privacy rights or any individual residing with you.

Laptop Regulations

1. Prior to the issuance of a laptop, staff must sign and agree to adhere to the Acceptable Use Policy. In addition, staff will be required to sign an acknowledgement when the laptop and its equipment are received.

2. The laptop is an educational tool and should be used in that capacity only. Any use of this educational technology and/or electronic communication that substantially disrupts or interferes with the orderly operation of the school or the rights of others will not be tolerated in or outside of the school facilities or school day. It may not be used to harass, intimidate or bully any person or persons. Any violation of law through the use of this technology may be dealt with through disciplinary action.

3. Once the laptop is issued, the staff member is responsible for it at all times. If the laptop or any of its components is suspected to be lost, staff must report it immediately to the main office and the Technology Department.

4. Laptops are subjected to recall at any time by district administration.

5. Keep all food and drinks away from the laptops.

6. Do not physically mark up the laptop or its storage case with wilting, stickers, etc.

7. Do not remove the inventory tag - if the tag becomes damaged and/or worn, please report it immediately to the Technology Department.

8. Keep laptop in its storage case when not in use to avoid damage.

9. The staff member is the only authorized user of their assigned laptop. Never share or swap laptops with another person unless directed by a school administrator.

10. There is a possibility files or data stored on the laptop may be deleted when it requires repair. Note: All data will be deleted when the laptop is returned at the end of the year. The staff member is responsible to save and backup any schoolwork or pertinent data.

11. Keep passwords confidential.

12. Use the laptop on a flat, stable surface.

13. Avoid touching the screen. When cleaning is necessary, wipe the laptop surface lightly with a soft cloth. Never use a cleaner, such as Windex or water, to clean laptop screens.

14. Do not rest pencils/pens or other items on the keyboard. Closing the laptop with items on the keyboard may accidentally damage the screen.

15. Do not insert objects into ports (openings) in the laptop that are not intended to be inserted.

16. Laptops are school district property. If a staff member fails to surrender their laptop prior to leaving the Springfield Public Schools District, that person will be in possessions of stolen property and charges will be filed.

Internet Safety Protection

As a condition for receipt of certain Federal funding, the school district shall be in compliance with the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and has installed technology protection measures for all computers in the school district, including computers in media centers/libraries. The technology protection must block and/or filter material and visual depictions that are obscene as defined in Section 1460 of Title 18, United States Code; child pornography, as defined in Section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, graphic image file or other material or visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

This Policy also establishes Internet safety policy and procedures in the school district as required in the Neighborhood Children's Internet Protection Act. Policy 2361 addresses access by minors to inappropriate matter on the Internet and World Wide Web; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; unauthorized access, including "hacking" and other unlawful activities by minors online; unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors.

Notwithstanding blocking and/or filtering the material and visual depictions prohibited in the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act, the Board shall determine other Internet material that is inappropriate for minors.

In accordance with the provisions of the Children's Internet Protection Act, the Superintendent or designee will develop and ensure education is provided to every student regarding appropriate online behavior, including students interacting with other individuals on social networking sites and/or chat rooms, and cyberbullying awareness and response.

The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly Board meeting or during a designated special Board meeting to address and receive public community input on the Internet safety policy - Policy and Regulation 2361. Any changes in Policy and Regulation 2361 since the previous year's annual public hearing will also be discussed at a meeting following the annual public hearing.

The school district will certify on an annual basis, that the schools, including media centers/libraries in the school district, are in compliance with the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act and the school district enforces the requirements of these Acts and this Policy.

N.J.S.A. 2A:38A-3
Federal Communications Commission: Children's Internet Protection Act
Federal Communications Commission: Neighborhood Children's Internet Protection Act

Adopted: 18 March 2019