

SPARTANBURG SCHOOL DISTRICT SEVEN

ACCEPTABLE USE POLICY

Policy IJNDB Technology Resources and Internet
Issued 6/12

Purpose

To establish the board's vision and the basic structure for the use of technology resources in instruction.

Technology is a vital part of education. In an effort to promote learning and expand educational resources for students, the district provides a variety of technology resources for students and staff.

The district's goal in providing these resources is to promote educational excellence by facilitating resource sharing, communication and innovation.

The purpose of the district's educational network is to support research and education in and among academic institutions by providing access to unique resources and the opportunity for collaborative work. All use of the Internet and network must be in support of education and research and consistent with the educational objects of the district. Use of other networks or computing resources must comply with the rules governing those networks. Transmission of any material in violation of any federal or state laws or regulations is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade secret. Access to computer systems and networks owned or operated by the district imposes certain responsibilities and obligations on users and is subject to district policies and local, state and federal laws.

Technology access

Because technology is a vital part of the educational process and the curriculum of the district, students and staff will be provided access to the Internet. By providing this access, the district intends to promote educational excellence in schools by allowing access to resources unavailable through traditional means. The district provides this instructional resource as an educational tool for staff and students and its use will be governed by this Internet acceptable use policy. The failure to follow this policy or responsibilities may result in the loss of privileges or other disciplinary measures. With access to computers and people all over the world also comes the availability of material that may not be of educational value in the context of the school setting. The district has taken precautions to restrict access to controversial or inappropriate materials; however, on a global network it is impossible to control access to all materials and an industrious user may discover controversial information. Users (and parents/legal guardians of the students who are users) must understand that neither the district nor any district employee controls the content available on outside systems. The district firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the district.

The smooth operation of the Internet network relies on the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided so that students and staff are aware of their responsibilities when using the Internet. All staff and students must abide by the generally accepted rules of network etiquette, including the following:

- Vandalism is prohibited. Vandalism includes any malicious attempt to harm or destroy data of others. Vandalism also includes, but is not limited to, the uploading or creation of computer viruses, deletion or alteration of other user files or applications, removing protection from restricted areas.
- Never access or attempt to access inappropriate or restricted information not directly related to educational purposes. Restricted information includes obscene, libelous, indecent, vulgar, profane or lewd materials, advertisements or services not permitted to minors by law; insulting, fighting and harassing words; and other materials which may cause a substantial disruption of the academic environment.
- Do not be abusive in messages to others. Profanity, vulgarities or other inappropriate language is prohibited. Illegal activities are strictly forbidden. Do not disrupt, harass or annoy other users.
- Documents, electronic mail, chat room messages and any other form of direct communications may not include a student's Social Security number or any other personally identifiable information that may lead to the identity of one's self or others. For example, do not reveal personal home addresses or phone numbers to others.
- No student pictures (video or still) or audio clips will be published without permission from the student's parent/legal guardian. No original student work will be published without permission from the student's parent/legal guardian.
- Electronic mail is not guaranteed to be private. People who operate the system have access to all electronic mail. Messages relating to or in support of illegal or inappropriate activities will be reported to the appropriate authorities.
- All communications and information accessible via the network should be assumed to be private property. Always cite all quotes, references and sources. Users may not reproduce copyrighted material without permission.
- All subject matter on district web pages will relate to curriculum, instruction, school-authorized activities or to the district. Neither students nor staff may publish personal home pages as part of district web sites or home pages for other individuals or organizations not directly affiliated with the district. All pages on the district's server(s) are property of the school district.
- Use of the Internet is for educational and educational support activities only. Users may not use the system for financial or commercial gain.
- All work should be proofread to avoid spelling and grammatical errors.

- Always follow the instructions of the supervising staff members.
- No user of the system may use the system to make an unauthorized disclosure or use of, or otherwise disseminate, personal identification information regarding minors and/or students.
- No user of the system may send messages or information with someone else's name on it or misrepresent the source of information entered or sent.
- No user of the system may distribute addresses, home phone numbers or other personal information which could then be used to make inappropriate calls or contacts.
- No user of the system may engage in "spamming" (sending an annoying or unnecessary message to large numbers of people).
- No user of the system may access or attempt to access and/or alter information in restricted areas of any network.
- No user of the system may download or load any software or applications without permission from the building network administrator or system administrator.
- No user of the system may violate the confidentiality rights of other users on any network.
- Failing to report abuses or other conditions that may interfere with the appropriate and efficient use of school resources will result in disciplinary actions.

Technology protection measures

In compliance with the Children's Internet Protection Act (CIPA), 47 USC § 254(h), the district uses technological devices designed to filter and block the use of any of the district's computers with Internet access to retrieve or transmit any visual depictions that are obscene, child pornography or "harmful to minors" as defined by the CIPA. Adult users of a district computer with Internet access may request that the "technology protection measures" be temporarily disabled for valid educational research purposes or other lawful purposes not otherwise inconsistent with this acceptable use policy.

Internet safety policy

Prior to accessing the Internet, students and staff must receive instruction on the appropriate use of the Internet. In addition, parents/legal guardians will be required annually to sign a permission form before students will be allowed access to the Internet. Students also must sign a form annually acknowledging that they have read and understand this policy, that they will comply with the guidelines set forth herein and that they understand the consequences for violating these guidelines. Employees must sign a similar acknowledgement form.

Email, phone and Internet usage

The district will monitor email, phone and Internet activity and may disclose the content and/or details when, in the district's sole discretion, there is a business need to do so. Employees and any students granted email accounts should not expect that email messages, even those marked as personal or accessed by a personal ID, are private or confidential.

Email, phone and Internet usage should be used only for business/educational purposes. The district reserves the right to monitor personal use to the same extent that it monitors business use. Use by employees of the district's communication system constitutes consent to monitoring. Continued use of the system is conditioned on acceptance of and strict adherence to the district's policies. Failure to adhere to policy requirements may result in discipline or dismissal.

Employees should exercise the same restraint and caution in drafting and transmitting email messages as when writing a formal memorandum on district or school letterhead. Users should assume that messages will be saved and reviewed by someone other than the original addressee.

Adopted 6/3/08; Revised 6/5/12

Legal references:

Federal law:

47 USC Section 254(h) - Children's Internet Protection Act.

The Digital Millennium Copyright Act of 1998, Section 512 - Limitations on liability relating to material online.

S.C. Code of Laws, 1976, as amended:

Section 10-1-205 - Computers in public libraries; regulation of Internet access.

Section 16-3-850 - Encountering child pornography while processing film or working on a computer.

Section 16-15-305 - Disseminating, procuring or promoting obscenity unlawful; definitions; penalties; obscene material designated contraband.

Section 59-19-90 - General powers and duties of school trustees.

Court cases:

Purdham v. Fairfax Co. Sch. Bd., 637 F.3d 421, 427 (4th Cir. 2011).