

Technology

The use of technology in the schools is a privilege and therefore must be used responsibly. Any student who fails to follow established technology rules will be disciplined according to the level of the offense. Principals and/or their designees will use their discretion in dealing with the severity of each offense within each level and in dealing with repeat offenders within any level.

Level One (1) Offense:

1. Verbal warning
2. Detention
3. Written warning with copy to principal or his/her designee and parent notification
4. Computer privileges revoked for a period of time to be determined by the administration

Level Two (2) Offense:

1. Parent notification and detention or in school suspension
2. Computer privileges revoked up to remainder of school year
3. Suspension

Level Three (3) Offense:

1. Suspension
2. Expulsion
3. Legal action

- Students are to use computers for educational purposes when given proper authorization and direct supervision by school personnel. (1)
- When logging into the network system or a local computer, all established entry procedures must be followed. Students are not to subvert entry systems. (1)
- Excessive printing or printing to unauthorized network printers is prohibited. (1)
- Students who login to the network or to a local computer must not leave their station unattended. They must log out when leaving the computer. Students will be held accountable and share in the disciplinary consequences of any inappropriate behavior that is tracked with their login ID. (1)
- Students are not to change classroom software configurations without authorized permission and direct supervision. This includes Windows systems and its icons and setups. (2)
- Students will be held accountable for damages incurred by faulty or virus-infected media including any removable media (disks, CDs, Zip, USB drives, etc.) (2)
- Students are not to utilize unauthorized login IDs or utilize other students' or school employees' login IDs. Students are not to give out IDs or passwords. All students will be held accountable and share in the disciplinary consequences of any inappropriate behavior that is tracked with their login ID. (2)
- Computer connections such as peripheral and network cables, power cords, and other wires are not to be disconnected without authorization and under direct supervision of school personnel. (2)

- Students are to adhere to SDPC Administrative Rule IFBGA-R. A copy begins on the following page. (2)
- Students are prohibited from using CD recordable or DVD recordable drives to duplicate copyrighted or intellectually protected materials. (2)
- Students are prohibited from downloading from the Internet any illegal or pirated copies of copyrighted or intellectually protected materials. (2)
- Students are not to access personal email, chat rooms and/or instant messaging unless directed to do so under the supervision of a teacher. (2)
- Students will not access unacceptable sites. (2-3)
- Students are not to tamper with the local computer or network operating system. (3)
- Students are not to install software of any kind. (3)
- Students are prohibited from direct contact with any fileserver, attached components, hubs, UPS, racks, wires, panels, etc. (3)
- Students must utilize printing, scanning, digitizing and video hardware appropriately. Inappropriate behavior includes: Printing, scanning, sending, or creating materials that are obscene, pornographic, offensive, threatening, or otherwise intended to harass or demean others. (3)
- Students are not to change computer or network configurations. Changes to the local computer or network system configurations are to be accomplished by approved district personnel. (3)
- Hardware defacement or destruction is a punishable offense that will include restitution. Students and their parents will be expected to pay for damages to hardware and software and the hourly costs of repair labor. This includes the use of magnets to destroy information, writing on equipment, disassembling parts, sticking objects in drives, peeling off labels, keyboard defacement, bending wires and cables, removing printer components, removing mouse roller balls, etc. (3)
- Students are not to copy district software or to download/utilize unlicensed software. (3)
- Students may not delete any files except their own personal files. (3)

USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

Code **IFBGA** Issued **3/06**

Technology is a vital part of education and the curriculum of the school district. In an effort to promote learning and expand educational resources for students, the district has made arrangements to provide access to technology resources contingent upon adherence to this policy, administrative rule and related guidelines. The School District of Pickens County will provide students and employees with access to the school district's technology resources including, but not limited to, computer systems, media and peripheral devices.

Access to the district's technological resources is a privilege, not a right. With this privilege, there also is a responsibility to use the resources solely for educational purposes and not to access inappropriate materials unsuitable for students. The school district's technology resources have specific educational purposes that include use for classroom activities, professional or career development and administrative functions. The faculty will thoughtfully integrate use of technology throughout the curriculum and will provide guidance and instruction to students in its use.

Use of the school district's technology resources is a privilege and is not intended to be a public forum. Student Internet activities will be monitored by the district to ensure students are not accessing inappropriate sites that have visual depictions that include obscenity, child pornography or are harmful to minors. The school district will use technology protection measures to protect students from inappropriate access.

The district will communicate its Internet acceptable use policy, administrative regulations and Internet safety measures annually through the student/parent handbook.

District and school computer technicians who are working with a computer and come across sexually explicit images of children must report this to local law enforcement and to the superintendent. The report must include the name and address of the owner or person in possession of the computer. Employees and students who violate the terms of the administrative rule related to the Internet will be subject to disciplinary action. Inappropriate use by any person will not be tolerated.

The School District of Pickens County will develop and implement administrative rules and regulations and user guidelines related to technological resources that are consistent with the purposes and mission of the district.

INTERNET

Code **IFBGA-R** Issued **3/06**

Internet access

Because technology is a vital part of the educational process, the curriculum of the school district, students and staff will be provided access to the Internet. By providing this access, the district intends to promote educational excellence and allow access to resources unavailable through traditional means. Through the Internet, students and staff may have access to a wide variety of educational resources.

With access to computers and people all over the world also comes the availability of material that may not be of educational value. The school district has taken precautions to restrict access to controversial or inappropriate materials. However, on a global network, it is impossible to control all materials and limit all access to information which has no educational value. The school district firmly believes that the valuable information and the interaction available on this worldwide network far outweigh the possibility that users may procure material that is not consistent with the educational goals of the school 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 here so that users will be aware of their responsibilities when using the Internet. Any violations of these guidelines will subject the user to appropriate disciplinary action and possible denial of access to the Internet.

Terms and conditions of use

Acceptable use

The purpose of the school district decision to provide Internet access is to allow an expanded opportunity for research and education by providing access to unique resources and the opportunity for collaborative work. All use of the Internet must be in support of education and research and consistent with the educational objectives of the school district. Use of other organizations' network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any national 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.

Procedures for use

Administrators and teachers may access the Internet for educational or work-related purposes at any time which is not disruptive and does not interfere with the performance of other responsibilities by the employee or other staff members.

Students will be allowed to access the Internet only through their teachers. No students may access the Internet without permission. Student use must be supervised at all times by a staff member.

Rules governing use

The use of the Internet is a privilege, not a right, and inappropriate use will result in cancellation of Internet privileges. All staff and students, when allowed use of the Internet and e-mail, must abide by the generally accepted rules of network etiquette, including the following.

- Be polite. Do not be abusive in communication to others. Always use appropriate language. Profanity, vulgarities or other inappropriate language is prohibited. Illegal activities are strictly forbidden.
- Never reveal the personal address or phone number of the user or others.
- Note that electronic mail is not guaranteed to be private. People who operate the system have access to all mail. Messages relating to or in support of illegal or inappropriate activities will be reported to the appropriate authorities.
- Do not disrupt, harass or annoy other users.
- All communications and information accessible via the network should be assumed to be private property. Always cite all quotes, references and sources.
- Never access inappropriate or restricted information, such as pornography or other obscene materials, or other information not directly related to the educational purposes for which access is being provided. Restricted information includes obscene, libelous, indecent, vulgar, profane or lewd materials; advertisements for products 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.
- Vandalism also is prohibited and will result in cancellation of privileges. Vandalism includes any malicious attempt to harm or destroy data of another user and includes, but is not limited to, the uploading or creation of computer viruses.
- All users should remain on the system only as long as necessary to complete their work, so that other individuals will have equal opportunities to access the Internet.
- All users should use the Internet only for research and academic reasons; non-academic uses are prohibited. Do not use the system for financial or commercial gain.
- Always follow the instructions of the supervising staff members.

Penalties for improper use

Employees

An employee who violates the terms of this administrative rule or otherwise misuses the Internet to access inappropriate material will be subject to disciplinary action, up to and including discharge. In addition, the privilege of accessing the Internet also will be subject to cancellation for up to one year.

Students

Students who violate the terms of this administrative rule or who otherwise misuse their access to the Internet also will be subject to disciplinary action in accordance with the district's student behavior code. Internet access privileges also may be canceled for up to one year.

Violations of the laws of the United States or the state of South Carolina also may subject the user to criminal prosecution.

If a user incurs unauthorized costs, the user, as well as the user's parents/legal guardians if the user is a student, will be responsible for all such costs.