Internet Safety and Network Acceptable Use

Access to the Internet/Network is a privilege, not a right. With this privilege, there also is a responsibility to use the Internet/Network solely for educational purposes and not to access materials not suitable for students. As part of the implementation of the administration's guidelines, students and staff must be instructed on the appropriate use of the Internet/Network. Inappropriate or disruptive use by any person will not be tolerated.

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/Network. Any violations of these guidelines will subject the user to appropriate disciplinary action and possible denial of access to the Internet/Network. In general, these guidelines require efficient, ethical, and legal utilization of the network resources.

In an attempt to protect students, the District has installed filtering/monitoring software to check Internet access by computer users on District equipment in compliance with the Children’s Online Privacy Protection Act. However, because access to the Internet/Network provides connections to other computer systems located all over the world, users (and parents of students who are users) must understand that neither the District nor any District employee can completely control the content of the information available on the systems. Every effort will be made by the District to monitor and restrict ready access to known objectionable sites; however, an industrious user may discover inappropriate or offensive information. The District does not condone the use of inappropriate or offensive materials and cannot be held responsible for such use.

Acceptable use

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 be consistent with the educational objectives 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.

Acceptable use is always ethical, reflects honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and the individual's rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance.

Procedures for use

1. 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.
2. Students will be allowed to access the Internet only through their teachers. Students may not 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/Network is a privilege, not a right, and inappropriate use will result in cancelation of Internet/Network privileges. All staff and students must abide by the generally accepted rules of network etiquette, including, but not limited to, the following:

1. Be polite. Do not be abusive, obscene, inflammatory, or threatening in messages to others. Always use appropriate language; profanity, vulgarities, or other inappropriate language is prohibited.
2. Documents 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 without proper parental consent. For example, do not reveal personal home addresses or phone numbers to others.
3. No student pictures (video or still) or audio clips will be published without written permission from the student's parent or guardian.
4. The District offers student Internet-based electronic mail accounts. The student accounts are intended for educational purposes. Users can access their e-mail from any computer that has Internet access. 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. All student e-mail accounts are filtered for inappropriate content. If for any reason a parent does not wish to have an e-mail account for his/her child, the parent should notify the principal in writing so that his/her child’s name can be removed from the e-mail accounts.
5. 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. Access to the Internet from District computers is filtered and monitored for inappropriate content through a software application.
6. All subject matter on District Web pages shall 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 District.
7. Vandalism is prohibited and will result, at a minimum, in cancelation of privileges. Vandalism includes any malicious attempt to harm or destroy data of another user, Internet, or other networks that are connected to any of the Internet infrastructures. 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, or the unauthorized blocking of access to information, applications, or areas of the network.
8. Do not share passwords. The only person who should ever use an account is the person to whom it belongs. Do not send messages or information with someone else's name on it.

The following list represents some inappropriate uses of the Internet, which are not permitted by the District, but by no means is this list intended to be exhaustive:

1. Commercial advertising, fundraising, or unethical/illegal solicitation.
2. Using copyrighted material without permission.
3. Sending or receiving messages or information that is inconsistent with the school's behavior code or assisting others to violate that code, including inappropriate, offensive, and/or disruptive messages or information.
4. Sending chain letters or engaging in "spamming" (sending an annoying or unnecessary message to large numbers of people).
5. Purchasing something which requires a credit card number or obligates a student or school to provide payment to another party.

6. Accessing, attempting to access, and/or altering information in restricted areas of any network.
7. Downloading or loading any software or applications without permission from the building network administrator or system administrator.

Users are required to report any of the following to their teachers, supervisors, or the building network administrator as soon as the following are discovered:

1. Any messages, files, Web sites, or user activities that contain materials that are in violation of this policy.
2. Any messages, files, Web sites, or user activities that solicit personal information, such as an address, phone number, credit card number, or social security number, about the user or someone else, or request a personal contact with the user or another user.
3. Attempts by any user to abuse or damage the system or violate the security of the network and its resources.
4. Any illegal activity or violation of school policy.
5. Any error messages or problems that indicate that the system is not working properly.

Penalties for improper use

An employee who violates the terms of this procedure or otherwise misuses the Internet to access or send 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 cancelation for a period of time as determined by the administration. Students who violate the terms of this procedure 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 a period of time as determined by the administration. 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 if the user is a student, will be responsible for all such costs.

Warranty

The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages suffered by any user. This includes loss of data resulting from delays, non-deliveries, misdirected deliveries, or service interruptions caused by the system's negligence, user errors, or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Security

Security on any computer system is a high priority, especially when the system involves many users. If you believe you have identified a security problem on the network, you must notify a staff member, Network System Administrator, Network System Analyst or Director of Technology. Do not demonstrate the problem to other users. Attempts to log on to any network as a system administrator or a person other than the user will result, at a minimum, in cancelation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be subject to severe restriction or cancelation of privileges.

User privacy

The District reserves the right to examine, restrict, or remove any material that is on or passes through its network, just as it does any other work or material generated or brought to school by staff or students. Access to electronic information related to any student or staff member will be governed by the same policies that would apply to that information if it were not in electronic form.

District policies

All documents on the District's servers must conform to District policies, as well as established school guidelines. Copies of District policies are available in all school offices. Persons developing or maintaining Web documents are responsible for complying with these and other policies. Some of the relevant issues and related policies include the following:

1. Electronic transmission of materials is a form of copying. As specified in District policy, no unlawful copies of copyrighted materials may be knowingly produced or transmitted via the District's equipment, including its Web server(s).
2. Documents created for the Web and linked to District Web pages will meet the criteria for use as an instructional resource.
3. Any links to District Web pages that are not specifically curriculum-related will meet the criteria established by the administration. Any other non-curricular materials should be limited to information about other youth activities, agencies, or organizations which are known to be non-sectarian, exclusively devoted to community interests or child welfare, non-profit, and non-discriminatory. Web page links may not include entities whose primary purpose is commercial or political advertising.
4. All communications via District Web pages will comply with this policy and the student behavior code. Offensive behavior that is expressly prohibited by this policy includes religious, racial, and sexual harassment and/or violence.
5. Any student information communicated via District Web pages will comply with District policies on Data Privacy and Public Use of School Records.

Changes in technical standards

Given the rapid change in technology, some of the technical standards outlined in this policy may require change throughout the year. Such changes will be made by the District network specialist with approval of the Superintendent. This Web page procedure may be updated on an annual basis, or more frequently if required.

Legal reference.

Federal.

13 U.S.C. 1301 et seq – Children’s Online Privacy Protection Act of 1998.