AR IJNDB-R Acceptable Use Of Technology Resources

Issued 6/12

Access

Because technology is a vital part of the educational process and the curriculum of the district, staff and students will be provided access to the district network, Internet, e-mail services and other technology resources. By providing this access, the district intends to promote educational excellence in schools by facilitating resource sharing, innovation, communication and learning. Through the district network, Internet and e-mail, students and staff will have access to the following.

- locally networked reference and research sources

- global information and news

- discussion groups on a vast range of topics

- local, regional, public, state and national library catalogs

- worldwide web

- electronic mail services

The availability of Internet access provides a unique educational opportunity for staff and students to contribute to the district's presence on the worldwide web. This medium of communication provides an opportunity to share accurate information with the community, our nation and the world about the district's curriculum and instruction, school-authorized activities and other related information. The district provides this instructional resource as an educational tool for staff and students.

The failure of an individual to adhere to the provisions of policy IJNDB, Acceptable Use of Technology Resources and its accompanying administrative rule will 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. The district firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material which is inconsistent with the educational goals of the school system.

The smooth operation of the network, Internet and e-mail services relies on the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided so that staff and students are aware of their responsibilities when using these technologies. In general, this requires efficient, ethical and legal utilization of the network resources.

Because access to the network provides connections to other computer systems located all over the world, users (and parents/legal guardians of students who are users) must understand that neither the district nor any district employee controls 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, the district does not condone the use of controversial or offensive materials and cannot be held responsible for such use.

Technology protection measures

In compliance with the Children's Internet Protection Act (CIPA), 47 U.S.C. § 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 in the CIPA. Adult users of a district computer with Internet access may request that the "technology protection measures" be temporarily disabled by the director of technology for bona fide research purposes or other lawful purposes not otherwise inconsistent with this administrative rule. The district will retain a copy of appropriate documentation demonstrating filter technology use for two years.

Internet safety policy

For purposes of this administrative rule, this is the district's "Internet safety policy." This administrative rule is designed to address access by minors to inappropriate matter on the Internet and worldwide web; the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications; unauthorized access, including so-called "hacking" and other unlawful activities by minors online; unauthorized disclosure, use and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors.

Annual responsibilities

Prior to accessing the district network, Internet or e-mail services, staff and students will receive instruction on the appropriate use of these services. Specifically, the district will provide annual education to students regarding appropriate online behavior, including interacting with other individuals via e-mail and on social networking sites, including in chat rooms, as well as cyber-bullying awareness and response. All students and parents/legal guardians must sign a form annually acknowledging that they have read and understand the district policy and administrative rule pertaining to use of technology resources, that they will comply with the policy and guidelines set forth herein, and that they understand the consequences for violating the policy and/or administrative rule. Documentation regarding this annual training will be maintained by the district for two years.

Terms and condition of use

Acceptable use

The purpose of the district network is to support research and education by providing access to unique resources and the opportunity for collaborative work. All use of the district network, Internet and e-mail services must be in support of education and research and consistent with the educational objectives of the district. Use of other networks or computing resources must comply with the guidelines 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, bullying and unwarranted annoyance.

Procedures for use

- Administrators and teachers may access the Internet or e-mail 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.

- With students, the district will notify parents/legal guardians about the district network, related safety issues and issues governing its Internet through a general letter/form to all parents/legal guardians during registration. Parental permission is not required for use of the Internet, but parents/legal guardians will be notified they have the right to file a parent/legal guardian denial form available during registration if they do not want their child(ren) to have access to Internet resources.

- Students must agree to the terms of the district's acceptable use policy in order to receive an individual, limited, school issued e-mail account (eChalk). The parent/legal guardian may withdraw approval at any time through a written request directed to the student's teacher or principal.

• All computer, Internet usage and e-mail usage by staff and students must be consistent with the board's mission and district policies. Students and staff members will not disclose, use or disseminate personal information about students in an unauthorized manner.

Rules governing use

Permitted uses of Internet and e-mail

Users will utilize e-mail for business purposes. Occasional personal use is permitted but the district reserves the right to monitor personal use to the same extent that it monitors business use.

Users may download text and other non-executable files attached to e-mail messages or from the Internet for school-related business only. Large files should be downloaded during off-peak hours whenever possible.

Users will check their e-mail frequently, delete unwanted messages promptly and stay within their e-mail quota. Be aware that the system administrator may delete e-mail at any time.

Users will subscribe only to high quality discussion group mail lists that are relevant to their educational or professional/career development.

General prohibitions

Users may not use the district system for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use. The district will not be responsible for any obligations resulting from any unauthorized use of the system.

Users may not use the system for political activities.

Users will not post chain letters or engage in spamming. Spamming is sending an unnecessary message to a large number of people.

Users will not attempt to obtain access to sites, areas or materials that are not authorized, whether or not such attempts are unlawful and whether or not such attempts may be deemed "hacking."

Personal safety

Students will not post or e-mail personal contact information about themselves or other people unless it is in conjunction with a specific teacher-approved assignment or approved college/career communication. Personal contact information includes address, telephone number, school address, etc.

Students will not agree to meet with someone they have met online without their parent/legal guardian's approval.

Students will promptly disclose to an administrator, teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

Illegal activities

Users will not attempt to gain unauthorized access to the e-mail system, the district web pages or any other computer systems through district e-mail and/or Internet and/or network access. Users will not attempt to perform functions that exceed their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal.

Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.

Users will not use the district system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of another person, or any other activity that violates existing district policies or procedures. Reference to such activities will not even be made in a joking manner or as a prank.

The district will notify law enforcement should illegal activities take place.

System security

Users will not share their account information (user ID and/or password) or attempt to log in to another user's account. Any sharing of user ID or password will result in immediate restriction or removal of account privileges. The only potential exception is the sharing of information with IT staff if requested for troubleshooting purposes.

Users will immediately notify the IT staff if they have identified a possible security problem. Students should notify a teacher and/or principal. Do not actively seek security problems but immediately report any potential issues that are found.

Users will not download or install any unauthorized software or install any unauthorized hardware.

Users will not run any executable files attached to an e-mail message.

Users will not knowingly use portable data storage devices which contain viruses or in any other way knowingly spread computer viruses.

Use of appropriate language

Restrictions against inappropriate language apply to public messages, private messages and material posted on web pages.

Users will not post or e-mail obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or gang-related language or symbols.

Users will not post or e-mail information which could cause damage or a danger of disruption.

Users will not post, email or engage in personal attacks, including prejudicial or discriminatory remarks.

Users will not harass another person. Harassment, which includes cyber-bullying, is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending message, he/she must stop immediately.

Users will not use any language in an e-mail that threatens another person, whether it is the recipient of the message or a third party.

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

Access to inappropriate material

Users will not use the district system to access or send material that is profane, lewd, vulgar, indecent, libelous or obscene, e.g., pornography, that advocates illegal acts, or that advocates violence or discrimination towards other people, e.g., hate literature.

Adult users who mistakenly access inappropriate information or images should immediately report this to an administrator. This will initiate proceedings to have the materials blocked. This will protect users against an allegation that they have intentionally violated the acceptable use of technology resources policy and administrative rule.

Students who mistakenly access inappropriate information or images should immediately report this to the attending teacher. The administration should be notified if it is deemed warranted. This will protect users against an allegation that they have intentionally violated the acceptable use of technology resources policy and administrative rule.

Students are expected to follow parental guidance regarding limitation of access to additional types of inappropriate materials.

Respect for privacy

Users will not post or e-mail private information about another person.

Penalties for improper use

A staff member who violates the terms of this policy and/or administrative rule or otherwise misuses e-mail or the Internet to access or send inappropriate material will be subject to disciplinary action, up to and including

termination from employment. In addition, the privilege of accessing the Internet and e-mail services also will be subject to cancellation. Students who

violate the terms of this policy and/or administrative rule or who otherwise misuse their access to e-mail or the Internet also will be subject to disciplinary action in accordance with the student behavior code. Internet and e-mail access privileges also may be cancelled. Violations of the laws of the United States or of the state of South Carolina also may subject student or employee users 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.

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 an employee or a student believes he/she has identified a security problem on the network, he/she must notify the administrator for the school. The employee or student will not demonstrate the problem to other users. Attempts to log on to any network as a system administrator will result in cancellation 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 restrictions, cancellation of privileges or other disciplinary and/or legal action.

User privacy

E-mail messages sent or received via a district-issued e-mail account and all other electronic files created using district resources or stored with district resources are property of the district.

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 staff member or student 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 server(s) must conform to district policies, rules and guidelines as well as established school guidelines. Copies of policies are available on the Internet at the district's webpage. Persons developing or maintaining web documents are responsible for complying with these and other policies. Some of the relevant issues and related district policies include the following.

- 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).

- Documents created for the web and linked to district web pages must meet the criteria for use as an instructional resource.

- Any links to district web pages that are not specifically curriculum-related must meet the criteria established in the acceptable use of technology resources policy and administrative rule. 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.

- All communications via district web pages will comply with the acceptable use of technology resources policy and administrative rule and the student behavior code. Offensive behavior that is expressly prohibited by this policy includes religious, racial and sexual harassment and/or violence.

• Any student information communicated via district web pages must comply with all other district policies.

Other

Material on a web page reflects an individual's thoughts, interests and activities. Such web pages do not, in any way, represent individual schools or the district and they are not endorsed or sanctioned by any individual school or the district. Concern about the content of any page(s) created by staff or students should be directed to the principal of that school or to that school's media specialist.

Given the rapid change in technology, some of the technical standards outlined in this administrative rule may require change throughout the year. Such changes will be made with approval of the superintendent. This administrative rule may be updated on an annual basis or more frequently as required or deemed necessary.

Issued 6/11/12