POLICY SERVICES ADVISORY

Volume 24, Number 2 June 2012

CONTENTS

Policy Advisory Discussion

Policy Advisory No. 440. IJNDB and IJNDB-R — Use of Technology Resources in Instruction.

In February of 2012 Policy Services provided policy advisory No. 436. In further review of the Federal Communications Commission (FCC), "Report and Order" we believe it is necessary to further adjust the language in Policy IJNDB. If advisory No 436 has been considered and approved by the district it is recommended the district consider and approve adjusted language found in PA 440. If the district has yet to consider and approve PA 436, it is best to forgo that approval and consider and approve PA 440.

The "Report and Order" adds the statutory language from the Protecting Children in the 21st Century Act regarding the education of students related to appropriate online behavior. This language adds to the current FCC rules implementing the Children's Internet Protection Act (CIPA).

The Protecting Children in the 21st Century Act establishes that E-rate applicants must certify that their CIPA required Internet safety policy provides for the education of students regarding appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and regarding cyberbullying awareness and response. Further there is a requirement that language is included related to monitoring the online activities of minors.

Specific procedures or curriculum for schools to use in the education of this matter is left to the discretion of each individual district to determine. Language included in the FCC "Final Rule" Appendix A of the "Report and Order" establishes that policy language must be adopted and enforced and must include a technology protection measure that protects against Internet access by both adults and minors to visual depictions that are obscene, child pornography or, with respect to use of the computers by minors, harmful to minors.

For further information refer to Federal Communications Commission document FCC 11-125.

It is important to remember that adjusted policy language needs to be in place immediately because it applies to the 2012-2013 funding year. It may, therefore, be in the best interest of the district to suspend the normal first and second reading defined in Policy BGB and move to adopt the adjusted language with one reading. Suspension of policy is defined in Policy BGF. Suggested agenda language for the suspension of policy in this instance is as follows:

> ***Agenda Item***: This agenda item provides the Governing Board an opportunity to discuss and consider the suspension of Board Policy BGB related to a first and second reading of recommended adjustments to Board Policy IJNDB, "Use of Technology Resources in Instruction"
>
> ***Discussion***: The Arizona School Boards Association has provided the District with adjusted language related to Board Policy IJNDB, Use of Technology Resources in Instruction. Due to the need to have this adjusted language in place for the 2012 E-rate funding year it is the recommendation of the administration that Board Policy BGB be suspended for agenda item _____ (*next agenda item number placed here*) of this agenda dated _____ (*board meeting date*). Doing so provides the Board the opportunity to consider adjustments to Policy IJNDB with one reading rather that the specified two readings noted in BGB. Authority for such action is provided in Board Policy BGF, Suspension/Repeal of Policy.
>
> ***Motion***: Move to suspend Governing Board Policy BGB related to a first and second reading, regarding policy adoption, for the discussion and consideration of agenda item _____ of this Board agenda dated _____.

It is important for the district to maintain related posting notifications, board agenda(s), and minutes of the board meeting(s) where this item is discussed and considered. It is also important for the district to maintain all financial records

related to the purchase and utilization of filtering software; the dissemination of related policy and regulation documents, along with documents such as employee handbooks, student handbooks and any related news letters or articles; and all related training. Such documentation should be maintained in compliance with by the Arizona State Library, Archives and Public Records retention schedule.

If there are questions, contact Policy Services at (602) 254-1100 or fax information to (602) 254-1177. Ask for Chris Thomas, General Counsel/Director of Legal/Policy Services; Dr. Terry Rowles, Policy Advisor; or Steve Highlen, Policy Analyst. E-mail addresses are, respectively, [cthomas@azsba.org], [trowles@azsba.org], and [shighlen@azsba.org].

USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

Appropriate use of Electronic Information Services

The District may provide electronic information services (EIS) to qualified students, teachers, and other personnel who attend or who are employed by the District. Electronic information services include networks (e.g., LAN, WAN, Internet), databases, and any computer-accessible source of information, whether from hard drives, tapes, compact disks (CDs), floppy disks, or other electronic sources. The use of the services shall be in support of education, research and the educational goals of the District. To assure that the EIS is used in an appropriate manner and for the educational purposes intended, the District will require anyone who uses the EIS to follow its guidelines and procedures for appropriate use. Anyone who misuses, abuses, or chooses not to follow the EIS guidelines and procedures will be denied access to the District's EIS and may be subject to disciplinary ~~action~~ and/or legal action.

The Superintendent shall determine steps, including the use of an Internet filtering mechanism, that must be taken to promote the safety and security of the use of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Technology protection measures shall protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography or, with respect to use of computers by minors, harmful to minors. Safety and security mechanisms shall include online monitoring activities.

As required by the Children's Internet Protection Act, the prevention of inappropriate network usage includes unauthorized access, including "hacking," and other unlawful activities; unauthorized disclosure, use and dissemination of personal identification information regarding minors.

It is the policy of the Board to:

- prevent user access over the District's computer network, or transmissions of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
- prevent unauthorized access and other unlawful online activity;

- prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

- comply with the Children's Internet Protection Act [P.L. No. 106-554 and 47USC 254(h)].

Each user will be required to sign an EIS user's agreement. The District may log the use of all systems and monitor all system utilization. Accounts may be closed and files may be deleted at any time. The District is not responsible for any service interruptions, changes, or consequences. The District reserves the right to establish rules and regulations as necessary for the efficient operation of the electronic information services.

The District does not assume liability for information retrieved via EIS, nor does it assume any liability for any information lost, damaged, or unavailable due to technical or other difficulties.

Filtering and Internet Safety

As required by the Children's Internet Protection Act, ~~T~~the District shall provide for technology protection measures that protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to use of the computers by students, harmful to students. The protective measures shall also include monitoring the online activities of students.

Limits, controls, and prohibitions shall be placed on student:

- access to inappropriate matter.

- safety and security in direct electronic communications.

- unauthorized online access or activities.

- unauthorized disclosure, use and dissemination of personal information.

~~**Monitoring and Online Behavior**~~

~~The District shall monitor online behaviors and provide all students with instruction related to appropriate online behaviors including interacting with other individuals on social networks and in chat rooms and cyberbullying awareness and response. The Superintendent shall develop and implement the District's instructional program and shall develop and implement the District's program for monitoring the use of District technologies.~~

Education, Supervision and Monitoring

It shall be the responsibility of all District employees to be knowledgeable of the Board's policies and administrative guidelines and procedures. Further, it shall be the responsibility of all employees, to the extent prudent to an individual's assignment to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

The Superintendent shall provide for appropriate training for District employees and for students who use the District's computer network and have access to the Internet. Training provided shall be designed to promote the District's commitment to:

- the standards and acceptable use of the District's network and Internet services as set forth in District policy;
- student safety in regards to use of the Internet, appropriate behavior while using, but not limited to, such things as social networking Web sites, online opportunities and chat rooms; and cyberbullying awareness and response; and compliance with E-rate requirements of the Children's Internet Protection Act.

While training will be subsequently provided to employees under this policy, the requirements of the policy are effective immediately. Employees will be held to strict compliance with the requirements of the policy and the accompanying regulation, regardless of whether training has been given.

The Superintendent is responsible for the implementation of this policy and for establishing and enforcing the District's electronic information services guidelines and procedures for appropriate technology protection measures (filters), monitoring, and use.

Adopted: date of Manual adoption

LEGAL REF.: A.R.S. 13-2316
13-3506.01
13-3509
15-341
34-501
34-502
20 U.S.C. 9134, The Children's Internet Protection Act
47 U.S.C. 254, Communications Act of 1934 (The Children's Internet Protection Act)

REGULATION REGULATION

USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

(Safety and use of Electronic Information Services)

Use of the electronic information services (EIS) requires that the use of the resources be in accordance with the following guidelines and support the education, research, and educational goals of the District. Filtering, monitoring, and access controls shall be established to:

- Limit access by minors to inappropriate matter on the Internet and World Wide Web.
- Monitor the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
- Monitor for unauthorized access, including so-called "hacking", and other unlawful activities by minors online.
- Restrict access by minors to materials harmful to minors.

Content Filtering

A content filtering program or similar technology shall be used on the networked electronic information services (EIS) as well as on standalone computers capable of District authorized access to the Internet. The technology shall at a minimum limit access to obscene, profane, sexually oriented, harmful, or illegal materials. Should a District adult employee have a legitimate need to obtain information from an access-limited site, the Superintendent may authorize, on a limited basis, access for the necessary purpose specified by the employee's request to be granted access.

Education, Supervision, and Monitoring

It is the responsibility of all District employees to be knowledgeable of the Board's policy and administrative regulations and procedures related to the use of technology resources. Employees are further responsible, to the extent prudent to an individual's assignment, to educate, supervise, and monitor student use of the District's online computer network use. District, department, and school administrators shall provide employees with appropriate in-servicing and assist employees with the implementation of Policy IJNDB.

As a means of providing safety and security in direct electronic communications and to prevent abuses to the appropriate use of electronic equipment, all computer access to the Internet through the District electronic information services (EIS) or standalone connection shall be monitored periodically or randomly through in-use monitoring or review of usage logs.

Access Control

Individual access to the EIS shall be by authorization only. Designated personnel may provide authorization to students and staff who have completed and returned an electronic information services user agreement. The Superintendent may give authorization to other persons to use the EIS.

Acceptable Use

Each user of the EIS shall:

- Use the EIS to support personal educational objectives consistent with the educational goals and objectives of the School District.
- Agree not to submit, publish, display, or retrieve any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.
- Abide by all copyright and trademark laws and regulations.
- Not reveal home addresses, personal phone numbers or personally identifiable data unless authorized to do so by designated school authorities.
- Understand that electronic mail or direct electronic communication is not private and may be read and monitored by school employed persons.
- Not use the network in any way that would disrupt the use of the network by others.
- Not use the EIS for commercial purposes.
- Follow the District's code of conduct.
- Not attempt to harm, modify, add, or destroy software or hardware nor interfere with system security.
- Understand that inappropriate use may result in cancellation of permission to use the educational information services (EIS) and appropriate disciplinary action up to and including expulsion for students.

In addition, acceptable use for District employees is extended to include requirements to:

- Maintain supervision of students using the EIS.
- Agree to directly log on and supervise the account activity when allowing others to use District accounts.
- Take responsibility for assigned personal and District accounts, including password protection.
- Take all responsible precautions, including password maintenance and file and directory protection measures, to prevent the use of personal and District accounts and files by unauthorized persons.

Each user will be required to sign an EIS user agreement. A user who violates the provisions of the agreement will be denied access to the information services and may be subject to disciplinary action. Accounts may be closed and files may be deleted at any time. The District is not responsible for any service interruptions, changes, or consequences.

Details of the user agreement shall be discussed with each potential user of the electronic information services. When the signed agreement is returned to the school, the user may be permitted use of EIS resources through school equipment.