# Board Policy

# 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 anything attached to, or delivered through our network (Local Access, Wide Area, Internet), or any computer accessible sources of information (hard drives, tapes, CDs, floppy disks, or other electronic sources). The uses 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 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. Each site will create and maintain an updated database of acceptable users. This list will be made accessible to all instructional staff.

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, 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 students, harmful to students.

Limits, controls and prohibitions shall be placed on students:

- access to inappropriate matter, including chat rooms
- safety and security in direct electronic communications
- unauthorized online access or activities
- unauthorized disclosure, use and dissemination of students' personal information

**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 technology protection measures (filters), monitoring and use.

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 (CIPA)

# 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 education, research and the educational goals of the School 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 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 the home addresses, personal phone numbers, or personally identifiable data of students or other employees unless authorized to do so by designated school authorities.

- Understand that electronic mail or direct electronic communication sent via the EIS is legally the property of the District. As such, it is not private, and becomes part of the public record. Messages may be read and monitored by school-employed persons, as well as the courts, newspapers and the general public. Non-confidential modes of communication should not be used to communicate confidential information.

- 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, copy, distribute or destroy software nor interfere with system security.

- Understand that many services and products are available for a fee and *acknowledge the responsibility for any expenses incurred without District authorization.*

- Understand that inappropriate use may result in cancellation of permission to use the EIS and appropriate disciplinary action, up to and including expulsion for students and dismissal for employees.

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.
- Prohibit the loading of personal, unauthorized software.
- 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.
- Prohibit unauthorized technology resources in the classroom including, but not limited to, personally-owned equipment, such as computers and printers, software, modems, and wired or wireless networking devices.

Each user will be required to sign an EIS user's 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 are not private, and may be monitored. Accounts may be closed and files may be deleted at any time. The District is not responsible for any service interruptions, changes, or consequences.

It is expected that each user will be responsible for reading, understanding and maintaining a copy of the user agreement. When the signed agreement is returned to the school or site, the user may be permitted use of EIS resources through the school or site equipment.

**Exhibit Exhibit Exhibit**

# USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

## ELECTRONIC INFORMATION SERVICES USER AGREEMENT

### I. General Terms and Conditions

Each user will be required to sign an EIS user's agreement. When the signed agreement is returned to the school, the user may be permitted use of the electronic information services (EIS) resources. Electronic information services include anything attached to, or delivered through our network (Local Access, Wide Area, Internet), any computer accessible sources of information (hard drives, tapes, CDs, floppy disks, or other electronic sources), and the School District phone system. Each user must:

- Use the EIS to support personal educational objectives consistent with the educational goals and objectives of the District.
- Not use the EIS for commercial purposes. No commercial business ventures may be advertised using our EIS (either via e-mail, electronic bulletin board or other electronic messaging system).
- Follow the District's code of conduct.
- Take responsibility for assigned District accounts, including password protection.
- Take all responsible precautions, including password maintenance and file and directory protection measures, to prevent the use of District accounts and files by unauthorized persons.
- Report any misuse of the EIS to the administration or system administrator, as appropriate.
- Understand that many services and products are available for a fee and *acknowledge the responsibility for any expenses incurred without District authorization.*
- Understand that inappropriate use may result in cancellation of permission to use the EIS and appropriate disciplinary action, up to and including expulsion for students and dismissal for employees.

Accounts may be closed and files may be deleted at any time. The District does not assume liability for any information lost, damaged, or unavailable due to technical or other difficulties, and is not responsible for any service interruptions, changes, or consequences.

The District specifically denies any responsibility for the accuracy of information retrieved via the EIS. While the District will make an effort to ensure access to proper materials, the user has the ultimate responsibility for how the EIS is used and bears the risk of reliance on the information obtained.

## II. Communications

Each user must:

- Not reveal the home addresses, personal phone numbers, or personally identifiable data of students or other employees unless authorized to do so by designated school authorities.
- Agree not to submit, publish, display, or retrieve any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.
- Understand that electronic mail or direct electronic communication is not private, and may be read and monitored by school-employed persons. Non-confidential modes of communication should not be used to communicate confidential information.
- Be polite, use appropriate language, and engage in appropriate online behavior. Users of the EIS should remember that they represent the School District in their communications and behavior. Users will not send, nor encourage others to send, abusive messages, nor engage in cyberbullying.

Definition: Cyberbullying is, but is not limited to, any act of bullying committed by use of electronic technology or electronic communication devices, including telephonic devices, social networking and other Internet communications, on school computers, networks, forums and mailing lists, or other District-owned property, and by means of an individual's personal electronic media and equipment. Cyberbullying may include threats, hate speech, ridicule or posting false statements as fact to humiliate a student.

## III. Hardware

Each user must:

- Not use the network in any way that would disrupt the use of the network by others.
- Not use unauthorized technology resources in the classroom.
- Not attempt to harm, modify, or destroy hardware nor interfere with system security.
- Not attempt to add unauthorized hardware.

## IV. Software and Electronic Content

Each user must:

- Abide by all copyright and trademark laws and regulations.
- Not attempt to harm, modify, add, or destroy software nor interfere with system security.
- Not load personal software.
- Not use the EIS to download media files (recorded audio, recorded video, multimedia) for non-instructional use.
- Not copy personal media files to the EIS for non-instructional use.

NOTE: Any use of media files (recorded audio, recorded video, multimedia) must follow ALL copyright regulations and ALL Fair Use guidelines. (If not **directly tied to the course curriculum**, the use of copyrighted materials may constitute copyright infringement. Copyright infringement is illegal, a violation of this acceptable use agreement, and is subject to litigation and prosecution.)

## V. Personal Devices

Each user must:

- Not attach unauthorized personal electronic devices to the EIS.

## VI. Additional Requirements for District Employees

District employees must:

- Maintain supervision of students using the EIS.
- Agree to directly log on and supervise the account activity when allowing others to use a District account.
- Prohibit students and others from loading personal software.
- Prohibit unauthorized technology resources in the classroom.
- 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.

I understand and will abide by the provisions and conditions indicated.  I understand that any violations of the above terms and conditions may result in disciplinary action and the revocation of my use of information services.

Name (printed) ____________________________________________________________________

Signature ____________________________________________________ Date _______________
(student or employee)

School ______________________________________ Grade (if a student) ___________________

*Note that this agreement applies to both students and employees*

The user agreement of a student who is a minor must also have the signature of a parent or guardian who has read and will uphold this agreement.

**Parent or Guardian Cosigner**

As a parent or guardian of the above named student, I have read this agreement and understand it.  I understand that it is impossible for the School District to restrict access to all controversial materials, and I will not hold the District responsible for materials acquired by use of the electronic information services (EIS).  I also agree to report any misuse of the EIS to a School District administrator.  (Misuse may come in many forms, but can be viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, or other issues described in the agreement).

I accept full responsibility for supervision if, and when, my child's use of the EIS is not in a school setting. I hereby give my permission to have my child use the electronic information services.

Parent or Guardian Name (print) ______________________________________________________

Signature ____________________________________________________ Date _______________