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.

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

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.

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

Adopted: November 8, 2001

LEGAL REF.: Public Law No. 106-554. Section 1721 of CIPA amends section 254(h) of the Communications Act of 1934, as amended, 47 U.S.C. § §151 *et seq*. Section 1721 references section 1732 of the Children's Internet Protection Act, which amends section 254 of the Communications Act by adding a new subsection (l) at the end of section 254. Sections 1731-1733 of CIPA are also referred to as the Neighborhood Children's Internet Protection Act (N-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 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 system (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.

Monitoring

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 systems (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 a 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.

EXHIBIT EXHIBIT

USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

ELECTRONIC INFORMATION SERVICES USER AGREEMENT

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.

Terms and Conditions

Acceptable use. Each user must:

- 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.

Personal responsibility. I will report any misuse of the EIS to the administration or system administrator, as is appropriate.

I understand that many services and products are available for a fee and *acknowledge my personal responsibility for any expenses incurred without District authorization.*

Network etiquette. I am expected to abide by the generally acceptable rules of network etiquette. Therefore, I will:

- *Be polite and use appropriate language.* I will not send, or encourage others to send, abusive messages.
- *Respect privacy.* I will not reveal any home addresses, or personal phone numbers or personally identifiable information.
- *Avoid disruptions.* I will not use the network in any way that would disrupt use of the systems by others.
- *Observe the following considerations:*
  - Be brief.
  - Strive to use correct spelling and make messages easy to understand.
  - Use short and descriptive titles for articles.
  - Post only to known groups or persons.

Services.

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

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 the 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_____