Southeast Local School District
Acceptable Use Policy

1. The network should not be used in such a way that it disrupts the use of the network by others such as, and not limited to:
   - Copying
   - Damaging or in any way altering any hardware or software
   - Introducing any form of computer virus

2. The user in whose name a network account is issued is responsible for its proper use at all times.
   - Users shall keep personal passwords, home addresses, and telephone numbers private
   - Users shall use this system only under their account issued by the District
   - Any problems arising from the use of a User's account are the responsibility of the account holder

3. Users will not use or aid in the misuse of another's files and directories, such as:
   - "Hacking"
   - Gaining unauthorized access to other computers or computer systems
   - Attempting to gain such unauthorized access

4. Obscene, pornographic, abusive, or other objectionable material which the district believes to be unlawful or inappropriate shall not be
   - Deliberately viewed
   - Download
   - Transmitted

   Users will not attempt, nor will user show others how to do these actions.

5. Use of technology tools, including games, is restricted to school related curriculum projects and must be supervised or approved by a teacher or administrator.

6. Users will not bring nor load any software or other programs onto any school computer.

7. Network users shall not violate any federal, state, or local criminal or civil laws. Network users shall not load, install, or disseminate copyrighted material or illegal copyrighted software onto or through the network. (Public domain and "Shareware" software and materials may be downloaded after permission is obtained from a teacher or administrator.)

8. Users will follow any other regulations, and netiquette posted in the labs or at any other computer workstation in individual buildings.

The District has implemented technology-blocking measures to prevent students from accessing inappropriate material on school computers. The District also has the ability to monitor Internet activity and reserves the right to do so. The District cannot guarantee that students can or will not get into undesirable or objectionable materials on the Internet because it is impossible to do so.

Annually, a student who wishes to have computer network and Internet access during the school year must read the Acceptable Use Policy and submit a properly signed agreement form. Students are asked to sign a new agreement each year after reviewing the policies and regulations of the District.

AUP Consequences

1st Degree Offenses

1st Consequence	No access for one calendar year
2nd Consequence	No access for the rest of the student's career in Southeast

2nd Degree Offenses

1st Consequence	A written warning with remediation
2nd Consequence	No access for 60 school days
3rd Consequence	No access for one calendar year

3rd Degree Offenses

1st Consequence	A written warning
2nd Consequence	No access for one week
3rd Consequence	No access for 30 school days
4th Consequence	No access for 60 school days

****

1. The network should not be used in such a way that it disrupts the use of the network by others

   1st or 2nd Degree, depending upon intent.

2. The user in whose name a network account is issued is responsible for its proper use at all times

   2nd Degree

3. Users will not use or aid in the misuse of another's files and directories

   2nd Degree

4. Obscene, pornographic, abusive, or other objectionable material which the district believes to be unlawful or inappropriate…

   1st Degree

5. Use of technology tools, including games, is restricted to school related curriculum projects…

   2nd Degree

6. Users will not bring nor load any software or other programs onto any school computer

   1st Degree

7. Network users shall not violate any federal, state, or local criminal or civil laws

   1st Degree

8. Users will follow any other regulations, and netiquette posted in the labs or at any other computer

   3rd Degree

Compliance With the Requirements of CIPA

(Children's Internet Protection Act)

Implementation of the following by July 1, 2002:

1. Employ A Technology Protection Measure

A Technology Protection Measure is a specific technology that blocks or filters Internet access. It must protect against access by adults and minors to visual depictions that are obscene, child pornography, or – with respect to use of computers with Internet access by minors – harmful to minors. It may be disable for adults engaged in bona fide research or other lawful purposes. For schools, the policy must also include monitoring the online activities of minors.

2. Adopt An Internet Safety Policy

The Internet Safety Policy must address the following issues:

- Access by minors to inappropriate matter on the Internet and World Wide 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 information regarding minors; and
- Measures designed to restrict minors' access to materials harmful to minors.

3. Public Notice and Hearing

The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing to address a proposed Technology Protection Measure and Internet Safety Policy.