SOUTHEAST DELCO SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: INTERNET ACCESS, ELECTRONIC MAIL, AND NETWORK RESOURCES ACCEPTABLE USE POLICY

ADOPTED: AUGUST 27, 2007

REVISED:

815. INTERNET ACCESS, ELECTRONIC MAIL, AND NETWORK RESOURCES ACCEPTABLE USE POLICY

1. Purpose

Internet access, electronic mail (e-mail), and network resources are available to district teachers, administrators, and students for educational and instructional purposes and other purposes consistent with the educational mission of the district. Use of the Internet, e-mail and network resources is a privilege.

With Internet and e-mail comes the availability of material that may not be considered appropriate in a school setting. The district cannot regulate and monitor all the information received or sent by persons who use the Internet or e-mail. The district cannot ensure that students who use the Internet or e-mail will be prevented from accessing inappropriate materials or sending or receiving objectionable communications. To the extent practical, steps shall be taken to promote the safety and security of users of the district online computer network, specifically, as required by the Children's Internet Protection Act.

To that end, this policy is designed to:

1. Ensure the security of all elements of Southeast Delco School District computer systems, related technology, and electronic information.

2. Delineate appropriate uses for all users of Southeast Delco School District computer systems.

3. Promote intellectual development through the use of computer systems, related technology, and electronic information in a safe environment.

4. Ensure compliance with relevant state, local, and federal law.

The responsibility for appropriate behavior rests with all individuals who use district information technology resources and computing facilities. Levels of access are provided depending on assignment, responsibility, and need to know. Users must protect information and resources against theft, malicious damage, unauthorized access, tampering, and loss.

2. Definitions	A computer system is hardware (laptops, both student and staff, LCD projectors, printers) software, and related technology including networks, wiring, and communications equipment. Electronic data are facts and information contained in any electronic form. Educational purposes are those actions directly promoting the educational, instructional, administrative, business, and support services mission of the district and related to any instruction, project, job, work assignment, task, or function for which the user is responsible. A user is any district staff member (including temporary), or student, authorized to use the district computer systems. Harmful to students means any text, graphic, pictorial, or auditory representation that taken as a whole and with respect to students, is pornographic or contains child pornography; or that advocates violence, and taken as a whole, lacks serious educational value to students including, but not limited to literary, artistic, political, or scientific value. Inappropriate materials consist of text, graphic, pictorial or auditory representations of items that are inconsistent with the educational mission of the district as set forth in Board policy, including material intended to teach skills that would enable an individual to engage in illegal activities, materials that promote discrimination against others based on race, religion, gender, nationality, sexual orientation, or advocate illegal use of any controlled dangerous substances or of alcohol. Filtering software (Filter) is software that is designed to limit access to selected portions of the Internet based on identified criteria. Its intended use is to limit access to inappropriate material and/or material that might be harmful to students. Internet access includes all methods used to connect to the Internet servers and users, and all methods for providing access regardless of funding or facilitating sources, including e-mail.
3. Authority 47 U.S.C Sec. 254	The Board shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors.

4. Guidelines	Monitoring The district reserves the right to log, monitor and review Internet, e-mail, and other network use of each user. This logging, monitoring and review may be conducted without cause and without notice. Each user of a district computer, by the use thereof, agrees and consents to such logging, monitoring and review and acknowledges that s/he has no right or expectation of confidentiality or privacy with respect to Internet, e-mail or other network usage. Network administrators may review student and staff files and communications to maintain system integrity and ensure that students and staff are using the system only for appropriate purposes. Users should expect that files stored on district servers or computers will not be private. The district does not maintain archives of all e-mail messages. Filter
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	The district shall employ the use of an Internet filter as a technology protection measure pursuant to law. Blocking shall be applied to visual depictions of materials deemed obscene or child pornography, or to any material deemed harmful to minors. The Filter may be disabled by the network administrator at the workstation level for use by an adult administrator or teacher for bona fide research or other lawful purposes. The Filter may not be disabled for use by students or other minors for any reason. Access Agreement All students, staff, administrators and teachers who use the Internet, e-mail and other network facilities must agree to and abide by all conditions of this policy. Each user must sign the Southeast Delco School District's Internet, Electronic Mail and Network Access Agreement which is attached to this policy. In the case of a student, the student's parent(s)/guardians(s) must sign the Agreement and Notice to Patents/Guardians. Students may not use the district's computers for access to the Internet or for e-mail without the approval or supervision of a teacher or district staff member. Prohibitions Use of the Internet, e-mail and network technology must be in support of the educational mission and instructional program of the district, in accordance with law and Board policy. All actions are subject to district review and may be logged. District e-mail is to be used for educational purposes only. Students are prohibited from using unauthorized e-mail, instant messaging and chat rooms.

	Although it is impossible to document all inappropriate conduct and use of computer facilities, the following guidelines provide examples of computer and network use infractions that are expressly prohibited with respect to all users: 1. System tampering (any unauthorized alteration of operating systems, individual accounts, software, networking facilities, and/or other programs) and/or equipment damage. 2. Decrypting passwords and/or gaining unauthorized higher level access or privileges or attempting to do so. 3. Interfering deliberately with other users. 4. Making statements or actions that are libelous, slanderous, discriminatory, threatening, or that harass others. 5. Using language that is obscene, vulgar, abusive, or otherwise harmful to students. 6. Knowingly introducing viruses or attempting to do so. 7. Reading, deleting, copying, forging, or modifying the e-mail of other users or attempting to do so. 8. Permitting others to use one's personal e-mail address, account, or password. 9. Using commercial advertising, chain letters, or noneducational games on district systems.
Pol. 814	10. Use which involves any copyrighted violation or the copying, downloading or distributing copyrighted material without the owner's permission, unless permitted in accordance with Board policy. 11. Posting personally identifiable information about students or staff without authorization. 12. Using district networks or computer systems for personnel gain or any illegal activities. 13. Use for commercial, private advertisement or for-profit purposes. 14. Use for lobbying or political purposes.

15. Hate mail, harassment, discriminatory remarks, threatening statements and other antisocial communications on the network.

16. Loading or use of unauthorized games, programs, files, music or other electronic media.

17. Use to access, view or obtain material that is obscene or pornographic or child pornography.

18. Use to transmit material likely to be offensive or objectionable to recipients.

19. Use to obtain, copy or modify files, passwords, data or information belonging to other users.

20. Use to misrepresent other users on the network.

21. Use of another person's e-mail address, user account or password.

22. Use to disrupt the work of other persons (the hardware or software of other persons shall not be destroyed, modified or abused in any way).

23. Use to infiltrate or interfere with a computer system and/or damage the data, files, operations, software or hardware components of a computer or system.

24. The unauthorized disclosure, use or dissemination of personal information regarding minors.

25. Use for purposes of accessing, sending, creating or posting, materials or communications that are: damaging to another's reputation, abusive, obscene, sexually oriented, threatening, contrary to district policy on harassment, and/or harassing, or illegal.

26. Use to invade the privacy of other persons.

27. Posting anonymous messages.

28. Use to read, delete, copy or modify the e-mail or files of other users or deliberately interfering with the ability of other users to send or receive e-mail.

29. Use while access privileges are suspended or revoked.

30. Any attempt to circumvent or disable the Filter or any security measure.

31. Use inconsistent with network etiquette and other generally accepted etiquette.

Students are prohibited from knowingly accessing or attempting to access inappropriate material or material that is harmful to students. Student use of the Internet will be monitored by various methods including, but not limited to, technology and direct supervision.

Students are prohibited from disclosing, using or disseminating any personal identification information of themselves or others.

All users are prohibited from knowingly accessing or attempting to access portions of the Internet that do not promote the educational, instructional, administrative, business or support services' purposes of the district, or is not related to any instruction, project, job, work assignment, task, or function for which the user is responsible.

Any student who identifies a portion of the Internet that contains inappropriate material or material that is harmful to students which has not been filtered/blocked is required to notify teacher or building administrator immediately.

Any staff who identifies or is informed of a portion of the Internet that contains inappropriate material or material that is harmful to students which has not been filtered/blocked through the technology protection measure (Filter) is required to contact the district systems administrator.

<u>Etiquette</u>

Users are expected to abide by the generally accepted rules of network etiquette. These include but are not limited to the following:

1. Be polite. Refrain from abusive, vulgar or inappropriate language in messages to others. District rules and policies for behavior and communicating apply.

2. Do not reveal personally identifying information including addresses or telephone numbers of others.

3. Recognize that e-mail is not private or confidential.

4. Do not use the Internet or e-mail in any way that would interfere with or disrupt its use by other users.

5. Consider all communications and information accessible via the Internet to be private property.

6. Respect the rights of other users to an open and hospitable technology environment, regardless of race, sexual orientation, color, religion, creed, ethnicity, age, marital status or handicap.

Security

Security on any computer system is a high priority, especially when the system involves many users. Each user is required to report any security problems to the system administrator. The problem is not to be demonstrated to other users.

Electronic Data Security -

Users may only access information and/or computer systems to which they are authorized and that they need for their assignments and responsibilities.

Users are responsible for their own accounts. Users cooperate in the protection of their accounts by changing passwords as required and keeping passwords strictly confidential.Users are expressly prohibited from sharing of accounts and passwords. Any violations that can be traced to an individual account name will be treated as the responsibility of the account owner.

User must log off all systems before leaving a computer or workstation or allowing the others to use it.

It is the responsibility of every user to be aware of and follow security procedures in accordance with this policy.

Users must secure their electronic data. (Note: sensitive files must be saved to a secure location such as an individual's network folder/directory or a removable disk or media that is then secured in a locked file cabinet.)

The district is not responsible for information that may be lost due to system failures or interruptions. Users should make backup copies and ensure they are stored in a secure place.

Physical Security -

Computer systems equipment must be located and maintained in a secure physical environment. Users are responsible for cooperating with physical security provisions for computers and related technology.

When staff members are not present to supervise the area, all areas (including permanent or temporary storage) housing valuable computer equipment must be secured.

Computer or related equipment may not be removed from district property without appropriate authorization.

Users must employ local accountability procedures to sign in or out any computer or related equipment. This equipment must be returned to school principal or office that owns it, prior to the user leaving the district.

The local equipment inventory will be maintained as accurately as possible. New equipment will be added when acquired. Users may not remove the inventory marking or tags from computers.

Lost and stolen equipment should be reported immediately to the building principal, the Southeast Delco School District Police Department and the Technology Office.

Systems And Applications Security -

Users should not install software or hardware, or disable or modify security settings or measures (such as anti-virus software) installed on any computer for any purpose without permission of the Director of Technology or a member of the technology staff.

Users must not change the system settings without permission of either the Director of Technology or member of the technology staff.

District software and applications may not be installed or copied to a nondistrict computer except as specified by licensing agreements.

Network Security -

The district is not responsible for all of the information found on networks outside of the district organization, including the World Wide Web. The district does not have control over information residing on other systems or Internet sites to which there is access through the district network. Some outside sites and systems may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.

Users are responsible for ensuring that access to or importation of material on networks is for educational purposes.

	Any material or information purposefully posted or linked from a district system or Internet site must be consistent with the educational purpose as defined in this policy. Users are responsible for abiding by the rules applicable to the computer system(s) they use, including those accessed over the Internet from district equipment. The only remote access approved for all users is to district web pages through the Internet and to the district e-mail system. Remote access to all other district computer systems is not permitted. <u>Safety</u> To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc. Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.
47 U.S.C. Sec. 254	Internet safety measures shall effectively address the following: 1. Control of access by minors to inappropriate matter on the Internet and World Wide Web. 2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications. 3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities. 4. Unauthorized disclosure, use, and dissemination of personal information regarding minors. 5. Restriction of minors' access to materials harmful to them. <u>Consequences Of Inappropriate Use</u>

Pol. 218, 233, 317	The user, whether a student or employee, shall be subject to appropriate discipline, including dismissal in the case of employees, and permanent expulsion in the case of students, in the event any one or more provisions of this policy is violated. In addition to disciplinary procedures, the user shall be responsible for damages to equipment, systems or software resulting from deliberate or willful acts. Illegal activities or use (for example, intentional deletion or damage to files or data belonging to others, copyright violations, etc.) may be reported to the appropriate legal authorities for possible prosecution. The district reserves the right to remove a user account from the network to prevent unauthorized or illegal activity. The use of the Internet and e-mail is a privilege, not a right. District administrative staff, as may be approved by the Board, will deem what is appropriate and inappropriate use and their decision is final. <u>Other Issues</u> The district makes no warranties of any kind, whether express or implied, for the service it is providing. The district is not responsible, and will not be responsible, for any damages, including loss of data resulting from delays, non-deliveries, missed deliveries, or service interruption. Use of any information obtained through the use of the district's computers is at the user's risk. The district disclaims responsibility for the accuracy or quality of information obtained through the Internet or e-mail. The district assumes no responsibility or liability for any charges incurred by a user. Under normal operating procedures, there will be no cost incurred. Subscriptions to listservs must be pre-approved by the district. A student may not download or install any commercial software, shareware, or freeware onto network drives or disks, unless s/he has specific, prior, written permission from a teacher or administrator. References:

	Child Internet Protection Act – 24 P.S. Sec. 4601 et seq U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777 Internet Safety – 47 U.S.C. Sec. 254 State Board of Education Regulations – 22 PA Code Sec. 403.1 Board Policy – 218, 233, 317, 818