UPPER MERION AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEMS AND NETWORK

ADOPTED: July 7, 2003

REVISED:

815. ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEMS AND NETWORK

1. Purpose

Upper Merion Area School District provides employees and students with access to the school district's electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means.

The electronic communications systems and network provide vast, diverse and unique resources. The Board will provide access to the school district's networks and systems and to the Internet for staff members and for students in order to locate material to facilitate learning and teaching through interpersonal communications, access to information, conduct research, and collaborate, i.e., to foster the educational purposes and mission of the school district.

For students and for staff, the school district's network and electronic communications systems are to be used primarily for school-related purposes and performance of job duties. Incidental personal use of school computers is permitted so long as such use does not interfere with the employee's job duties and performance, with network and system operations, or with other system users. Personal use must comply with this policy and all other applicable policies, procedures and rules, and must not violate any of the rules contained in this policy, and must not damage the school's hardware, software, computer or electronic communication systems. The Board will also provide access to staff and faculty for accomplishing school district business.

School librarians, teachers, and staff will work together to help students develop critical thinking skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information to meet educational goals that are consistent with the school district's strategic plan and student learning outcomes.

2. Definitions
20 U.S.C.
Sec. 6777(e)(2)

Access to the Internet - A computer shall be considered to have access to the Internet if the computer is equipped with a modem or is connected to a computer network which has access to the Internet.

18 U.S.C. Sec. 2256(8)	**Child Pornography** - Any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: 1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. 2. Such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct. 3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 4. Such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.
20 U.S.C. Sec. 6777(e)(1)	**Computer** - Includes any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with a computer. Computer includes, but is not limited to: desktop, notebook, powerbook or laptop computers; specialized electronic equipment used for students' special educational purposes; global position system (GPS) equipment; personal digital assistants (PDAs); cell phones with or without Internet access and/or recording capabilities, mobile phones, or wireless devices; beepers; and any other such technology developed. **Electronic Communications Systems** - Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes. Further, an electronic communications system means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. Examples include, but are not limited to, the Internet, intranet, electronic mail services, GPS systems, cell phones and PDAs. **Educational Purpose** - Includes use of the network and electronic communications systems for classroom activities, professional or career development, and to support the school district's curriculum, policy and mission statement.

20 U.S.C. Sec. 6777(e)(6), 9134(f)
47 U.S.C. Sec. 254(h)

Harmful to Minors - Any picture, image, graphic image file or other visual depictions that:

1. Taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex, or excretion.

2. Depicts, describes, or represents in a patently offensive way with respect to what is suitable, for an actual or simulated sexual act or sexual content, actual or simulated normal or perverted sexual acts, or lewd exhibition of genitals.

3. Taken as a whole lacks serious literary, artistic, political, or scientific value as to minors.

Incidental Personal Use - Use by an individual employee for occasional personal communications. Personal use must comply with this policy and all other policies, procedures and rules, and may not interfere with the employee's job duties and performance, with the system operations, or with other system users. Under no circumstances should the employee believe his/her use is private, the school district reserves the right to monitor access and use of its network and electronic communications systems.

The School District Network - All components necessary to effect its operation, including, computers, copper and fiber cabling, wireless communications and links, equipment closets and enclosures, network electronics, telephone lines, printers and other peripherals, storage media, software, and other computers and/or networks to which the school district network may be connected, such as the Internet or those of other institutions.

20 U.S.C. Sec. 6777(e)(4)
47 U.S.C. Sec. 254(h)

Minor - An individual who has not attained the age of seventeen (17).

18 U.S.C. Sec. 1460

Obscene - Analysis of the material meets the following elements:

1. Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest.

2. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically designed by the applicable state or federal law to be obscene.

	3. Whether the work taken as a whole lacks serious literary, artistic, political, or scientific value.
18 U.S.C. Sec. 2246(2),(3) 18 Pa. C.S.A. Sec. 5903	**Sexual Act and Sexual Contact** - As defined at 18 U.S.C. § 2246(2), at 18 U.S.C. § 2246(3), and at 18 Pa. C.S.A. § 5903.
20 U.S.C. Sec. 9134(f) 47 U.S.C. Sec. 254(h)	**Technology Protection Measure(s)** - A specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.
18 U.S.C. Sec. 1460, 2256	**Visual Depictions** - Undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image but does not include mere words.
3. Authority	Access to the school district's electronic communications systems and networks through school resources is a privilege, not a right. Inappropriate, unauthorized, and illegal use may result in the revocation of those privileges and/or appropriate disciplinary action. The electronic communications systems and network and the user accounts are the property of the school district which reserves the right to deny access to prevent further unauthorized, inappropriate or illegal activity. The school district will cooperate fully with Internet Service Providers, local, state and federal officials in any investigation concerning or related to the misuse of the network and communications electronic systems. It is often necessary to access user accounts in order to perform routine maintenance and security tasks; system administrators have the right to access by interception, and the stored communication of user accounts for any reason in order to uphold this policy and to maintain the system. Electronic communications systems and network users have no privacy expectation in the contents of their personal files or any of their use of the school district's network or systems. The school district reserves the right to track, log and monitor network and system use and to monitor and allocate fileserver space.
P.L. 106-554 Sec. 1711, 1721	The school district reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through software blocking or general policy. Specifically, the school district operates and enforces technology protection measure(s) that monitor and track online activities of minors on its computers used and accessible to adults and students so as to filter or block inappropriate matter on

the Internet. **Inappropriate matter** includes visual, graphic, text and any other form of obscene, child pornography, or other material that is harmful to minors, hateful, illegal, defamatory, harassing, violent and terroristic. Measures designed to restrict adults' and minors' access to material harmful to minors may be disabled to enable an adult to access bona fide research or for another lawful purpose.

The school district reserves the right to restrict or limit usage of lower priority network, electronic communications systems and computer uses when network and computing requirements exceed available capacity according to the following priorities:

1. Highest - uses that directly support the education of the students.

2. Medium - uses that indirectly benefit the education of the students.

3. Lowest - uses that include reasonable and limited educationally-related interpersonal communications and incidental personnel communications.

4. Forbidden - all activities in violation of this policy.

The school district additionally reserves the right to:

1. Determine which network and electronic communications systems services will be provided through school district resources.

2. View and monitor network traffic, fileserver space, processor, and system utilization, and all applications provided through the network and communications systems, including e-mail.

3. Remove excess e-mail or files taking up an inordinate amount of fileserver disk space after a reasonable time and after notification to the user.

4. Log Internet, network, and electronic communications systems use by students and staff.

5. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and any other applicable school district policies occurs or state or federal law is violated, including, but not limited to, those governing network use, copyright, security, discipline and vandalism of school district resources and equipment.

	Due to the nature of the Internet as a global network connecting thousands of computers around the world, inappropriate materials, including those which may be defamatory, inaccurate, obscene, profane, pornographic, offensive, and illegal, can be accessed through the network and electronic communications systems. Because of the nature of the technology that allows the Internet to operate, the school district cannot completely block access to these resources. Accessing these and similar types of resources may be considered an unacceptable use of school resources and will result in suspension of network and electronic communications systems privileges and disciplinary action as outlined in appropriate school district policies.
4. Delegation of Responsibility	Through a program of education, the school district will educate students and teachers regarding their individual responsibility to refrain from engaging in this and other unacceptable uses of the network and electronic communication systems and the consequences of their actions if they do so. The Coordinator of Technology will serve as the coordinator to oversee the school district network and electronic communications systems and will work with other regional or state organizations as necessary. In conjunction with the Coordinator of Technology, the Assistant Superintendent will serve as the coordinator for the school district network and electronic communications systems, will approve activities, ensure teachers receive proper training in the use of the network and electronic communications systems and the requirements of this policy, establish a system to ensure adequate supervision of students using the network and electronic communications systems, maintain executed user agreements, and be responsible for interpreting the school district Acceptable Use of the Electronic Communications Systems and Network Policy at the student and staff level. The Coordinator of Technology will establish a process for setting-up individual and class accounts, set quotas for disk usage on the system, establish a retention schedule, and establish the school district virus protection process. Unless otherwise denied for cause, student access to the Internet, e-mail, or other network and electronic communications systems resources shall be through supervision by the professional staff. Administrators, teachers and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of these resources. All users have the responsibility to respect the rights of all other users within the school district and school district networks, electronic communications systems, and throughout the Internet, and to abide by the rules established by the school district and their Internet Service Providers.

	Limitation of Liability The electronic information available to students and staff does not imply endorsement of the content by the school district, nor does the school district guarantee the accuracy of information received via the Internet. The school district shall not be responsible for any information that may be lost, damaged, delayed, misdelivered, or unavailable when using the network and electronic communications systems. Neither shall the school district be responsible for material that is retrieved by the Internet, or the consequences that may result from them. The school district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet, network, and electronic communications systems. In no event shall the school district be liable to the user for any damages whether direct, indirect, special or consequential, arising out of the use of the Internet, network and electronic communication systems.
5. Guidelines	Access to the Network and Electronic Communications Systems Network and electronic communications systems user accounts will be used only by the authorized owner of the account for its authorized purpose. An account will be made available according to a schedule developed by appropriate school district authorities given the capability of school district hardware. Types of services included, but are not limited to: 1. School District System - The school district's Acceptable Use of the Electronic Communications Systems and Network Policy will govern all use of the school district network and electronic communications systems. Student use of the network and electronic communications systems will also be governed by the other relevant school district policies. 2. World Wide Web - All school district employees and students will have access to the web through the school district's networked computers and electronic communications systems. 3. E-Mail - School district employees will be provided with an individual account. 4. Guest Accounts - Guests may receive an individual account with the approval of a school district administrator if there is a specific, school district-related purpose requiring such access. Use of the electronic communications system by a guest must be specifically limited to the school district-related purpose. An agreement will be required and parental signature will be required if the guest is a minor.

Parental Notification and Responsibility

The school district will notify the parents about the school district network and electronic communications systems and the policies governing their use. This policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the school district to monitor and enforce a wide range of social values in student use of the Internet. Further, the school district recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. The school district will encourage parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the school district system. Parents are responsible for monitoring their children's use of the school district's networks when they are accessing the system from home.

School District Limitation of Liability

The school district makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the school district network and communications systems will be error-free or without defect. The school district will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The school district is not responsible for the accuracy or quality of the information obtained through or stored on the network and electronic communications systems. The school district will not be responsible for financial obligations arising through the unauthorized use of the school district's resources. See also Delegation of Responsibility, subsection Limitation of Liability, which shall be interpreted in conjunction with and as consistent with this subsection.

Prohibitions

The use of the Internet computer network and electronic communications systems for illegal, inappropriate, unacceptable, or unethical purposes by students or employees is prohibited. All users are strictly prohibited from engaging in the activities listed below. The school district reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the network and electronic communications systems.

These prohibitions are in effect any time school district resources are accessed whether in school, directly from home, or indirectly through another Internet Service Provider.

General Prohibitions –

It is prohibited to use the network and electronic communications systems to/for:

1. Non-work or non-school related communications, unless the use comports with this policy's definition of incidental personal use.

2. Access indecent, obscene, pornographic, child pornographic or terroristic material.

3. Transmit material likely to be offensive or objectionable to recipients, including, but not limited to, that which may be defamatory, inaccurate, obscene, lewd, vulgar, rude, inflammatory, threatening, profane, pornographic, offensive, terroristic and/or illegal.

4. Access or transmit gambling, pools for money, including but not limited to, basketball and football, or any other betting or games of chance.

5. Participate in discussion or news groups which cover inappropriate and/or objectionable topics or materials, including those which may be defamatory, inaccurate, obscene, profane, pornographic, offensive, terroristic and/or illegal.

6. Send terroristic threats, hate mail, harassing communications, discriminatory remarks, and offensive or inflammatory communications.

7. Participate in unauthorized Internet Relay Chats, instant messaging communications and Internet voice communications (online; real-time conversations) that are not for school-related purposes or required for staff members to perform their job duties.

8. Facilitate any illegal activity.

9. Communicate through e-mail for non-educational purposes or activities, unless it is for incidental personal use as defined in this policy. The use of e-mail to mass mail non-educational or non-work related information is expressly prohibited (i.e. the use of the "everyone" distribution list, building level distribution lists, or other e-mail distribution lists to offer personal items for sale is prohibited).

	10. Commercial, for-profit, or business purposes (except where such activities are otherwise permitted or authorized under applicable school district policies), unauthorized fundraising or advertising on behalf of the school district and non-school school district organizations, reselling of school district computer resources to non-school school district individuals or organizations, or unauthorized use of the school district's name. **Commercial purposes** is defined as offering or providing goods or services or purchasing goods or services for personal use. School district acquisition policies will be followed for school district purchase of goods or supplies through the school district system. 11. Political lobbying. School district employees and students may use the system to communicate with their elected representatives and to express their opinion on political issues. 12. Advertising of any kind, unauthorized fundraising or unauthorized use of the school district's name will not be permitted on the Internet or e-mail, or any other online service.
Pol. 814	13. Anything that results in a copyright violation. 14. Install, distribute, reproduce or use unlicensed software on school district computers, or to copy school district software to unauthorized computer systems. The authority to install software on school district computers is restricted to the Coordinator of Technology, the school district Computer Technicians, the Librarians, and the Computer Lab Aides. 15. Install computer hardware, peripheral devices, network hardware, or system hardware. The authority to install hardware is restricted to the Coordinator of Technology, the school district Computer Technicians, the Librarians, and the Computer Lab Aides. 16. Intentionally infringing upon the intellectual property rights of others. 17. Use of the network and electronic communications systems to commit plagiarism. 18. Making available material or information the possession or distribution of which is illegal. 19. Unauthorized access, interference, possession, or distribution of confidential or private information.

20. Intentionally compromising the privacy or security of electronic information.

21. Posting personal web pages without administrative approval.

22. Using the systems to send any school district information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the school district's business or educational interests.

23. Sending unsolicited commercial e-mail messages, also known as spam.

Access and Security Prohibitions –

Users must immediately notify the Coordinator of Technology if they have identified a possible security problem. The following activities related to access to the school district's computer network, electronic communications systems and the Internet are prohibited:

1. Misrepresentation (including forgery) of the identity of a sender or source of communication.

2. Acquiring or attempting to acquire passwords of others or giving your password to another.

3. Revealing a password or otherwise permitting the use of others (by intent or negligence) of personal accounts for computer, electronic communications systems, and network access.

4. Using or attempting to use computer accounts of others; these actions are illegal, even if only for the purposes of "browsing."

5. Altering a communication originally received from another person or computer with the intent to deceive.

6. Use of the school district resources to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, and being involved in a terroristic threat against any person or property.

7. Disabling virus protection software or procedures.

Operational Prohibitions –

The following operational activities and behaviors are prohibited:

1. Interference with or disruption of computer, electronic communications systems, or network accounts, services or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses," the sending of electronic chain mail, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts. In other words, the user may not hack or crack the network electronic communications systems, or others' computers, whether by parasiteware or spyware designed to steal information, or viruses and worms or other hardware or software designed to damage computers, the network, or any component of the network, or strip information, or completely take over a person's computer.

2. Altering or attempting to alter files, system security software or the systems without authorization.

3. Unauthorized scanning of the electronic communications systems and network for security vulnerabilities.

4. Attempting to alter any school district computing or networking components (including, but not limited to, fileservers, bridges, routers, or hubs) without authorization or beyond one's level of authorization.

5. Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer, electronic communications systems, or network services.

6. Connecting unauthorized hardware and devices to the electronic communications systems and network.

7. Loading, downloading, or use of unauthorized games, programs, files, or other electronic media.

8. Intentionally damaging or destroying the integrity of electronic information.

9. Intentional destruction of school district computer hardware or software.

10. Intentionally disrupting the use of electronic communications systems, networks or information systems.

11. Negligence leading to damage of school district electronic information, computing, electronic communications systems, or networking equipment.

12. Failure to comply with requests from appropriate teachers or school district administrators to discontinue activities that threaten the operation or integrity of computers, systems, or networks.

Content Guidelines

Information electronically published on the school district's electronic communications systems and network, including, but not limited to the school district's World Wide Web pages shall be subject to the following guidelines:

1. Published documents, web pages, electronic communications, or video conferences may not include a child's phone number, street address, or box number, name (other than first names) or the names of other family members.

2. Documents, web pages, electronic communications, or videoconferences may not include information which indicates the physical location of a student at a given time other than attendance at a particular school or participation in school activities.

3. Documents, web pages, electronic communications, or videoconferences may not contain objectionable material or point directly or indirectly to objectionable materials.

Pol. 814

4. Documents, web pages, and electronic communications must conform to school district policies and guidelines, including the copyright policy.

5. Documents to be published on the World Wide Web must be edited and approved according to school district procedures before publication.

Due Process

The school district will cooperate fully with the school district's Internet Service Provider, local, state, and federal officials in any investigation concerning or relating to any illegal activities conducted through the school district electronic communications systems and network.

In the event there is an allegation that a student has violated the school district's policy, the student will be provided with a written notice of the alleged violation and an opportunity to be heard in the manner set forth in the Student Disciplinary Code.

Pol. 218	Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic communications systems and network. If the alleged violation also involves a violation of other provisions of the Student Disciplinary Code, the violation will be handled in accordance with the applicable provision of the Student Disciplinary Code.
Pol. 317, 417, 517	Employee violations of this policy will be handled in accord with school district employee discipline policy. The school district may terminate the account privileges of a guest user by providing notice to the user. Guest accounts not active for more than thirty (30) days may be removed, along with the user's files without notice to the user. <u>Search and Seizure</u> User violations of the school district's acceptable use policy, the Student Disciplinary Code, school district employee discipline policy or the law may be discovered by routine maintenance and monitoring of the school district system, or any method stated in this policy, or pursuant to any legal means. The school district reserves the right to monitor any electronic communications, including but not limited to, Internet access, PDA use, and e-mails. Students and employees should not have the expectation of privacy in electronic communications, even when used for personal reasons. <u>Copyright Infringement and Plagiarism</u> Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the school district resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Teachers will instruct students to respect copyright, request permission when appropriate, and comply with license agreements.
P.L. 94-553 Sec. 107 Pol. 814	Violations of copyright law include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over computer networks, deep-linking and framing into the content of others' websites. Further, the illegal installation of copyrighted software or files for use on the school district's computers is expressly prohibited. This includes all forms of licensed software – shrink-wrap, clickwrap and electronic software downloaded from the Internet.

School district guidelines on plagiarism will govern use of material accessed through the school district's electronic communications systems and network. Users will not plagiarize works that they find on the Internet. Teachers will instruct students in appropriate research and citation practices.

Selection of Material

Board policies on the selection of materials will govern use of the Internet.

When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers will preview the materials and web sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the web site. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

School District Web Site

School District Web Site –

The school district will establish and maintain a web site and will develop web pages that will present information about the school district. The Coordinator of Technology and his/her staff will be responsible for maintaining the server and making sure the site is available on the Internet. Administrative department heads and building principals, or their designees, will be responsible for providing and updating the content of the web site.

School District Web Pages –

The school district will establish and maintain web pages that present information about the schools or class activities. The Coordinator of Technology and his/her staff will be responsible for maintaining the server and making sure the site is available on the Internet. Teachers, coaches, activity sponsors, department chairpersons and building principals, or their designees, will be responsible for providing and updating the content of the web site.

Safety

To the extent possible, users of the Internet, electronic communications systems, and network will be protected from harassment or unwanted or unsolicited communication. Any user who receives threatening or unwelcome communications shall immediately bring them to the attention of a teacher or administrator.

Users will not post personal contact information about themselves or other people, in other words, the user may not steal another's identity in any way, may not use spyware, parasiteware, cookies, or use the network in any way to invade privacy. Additionally, the user may not disclose, use or disseminate personal information of other students or employees (examples include, but are not limited to, student grades, social security numbers, home addresses, telephone numbers, school addresses, work addresses, credit card numbers, health and financial information, evaluations, psychological reports, and educational records). **Personal contact information** includes address, telephone, school address, and work address.

Student users will agree not to meet with someone they have met online unless they have parent consent.

Documents or videotapes may not include information which indicates the physical location of a student at a given time other than attendance at a particular school or participation in school activities.

Consequences for Inappropriate Use

Students and employees must be aware that violations of this policy or unlawful use of the computers, Internet or school district electronic communications systems and networks may result in disciplinary actions, or loss of privileges.

Loss of Internet, electronic communications systems, and network access could be one of the disciplinary actions, however this policy incorporates all other relevant school district policies, such as, but not limited to, the student and professional employee discipline policies, copyright policy, web site policy, property policies, curriculum policies, sexual harassment policy and terroristic threat policy.

General rules for behavior and communications apply when using the Internet, electronic communications system and network, in addition to the stipulations of this policy. Loss of access and other disciplinary actions may result from inappropriate use. For example, disciplinary action may be taken for inappropriate language or behavior in using the school district's resources.

The network user shall be responsible for damages to network, equipment, electronic communications systems, and software resulting from deliberate and willful acts. The user will also be responsible for incidental or unintended damage resulting from willful or deliberate violations of this policy.

Violations as described in this policy may be reported to the appropriate legal authorities, whether the Internet service provider, local, state, or federal law enforcement. The school district will cooperate to the extent legally required with authorities in all such investigations.

Vandalism will result in cancellation of access to the school district's Internet, electronic communications systems and network resources.

P.L. 94-553
Sec. 107

P.L. 106-554
Sec. 1711, 1721, 1732

20 U.S.C.
Sec. 6777