

ALLENTOWN SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF
COMMUNICATIONS AND
INFORMATION (CIS) SYSTEMS

ADOPTED: June 21, 2007

REVISED:

<p>1. Purpose</p>	<p style="text-align: center;">815. ACCEPTABLE USE OF CIS SYSTEMS</p> <p>The district provides employees, students, School Board members, authorized independent contractors, and district consultants with access to the district’s electronic communication systems and network, which may include Internet access.</p> <p>Computers, network, Internet, electronic communications and information systems, collectively called “CIS” systems, provide vast, diverse and unique resources. The Board provides access to the district’s CIS systems for users in order to access information, research, and collaboration to facilitate learning and teaching to foster the district’s educational purpose and mission.</p> <p>For users, the district’s CIS systems must be used primarily for education-related purposes and performance of school district job duties. Incidental personal use of school computers is permitted for employees as defined in this policy.</p> <p>CIS systems may include computers which are located or installed on district property or which have been brought onto a district location by an employee or student. The personal technology devices brought onto district property by employees and students which are suspected of containing district information, may be legally accessed to ensure compliance with this policy and other district policies to protect district resources, and to comply with federal and state law. Employees and students may not use their personal computers to access the district’s Intranet, Internet or any other CIS system unless approved by the Superintendent and/or designee.</p> <p>The district intends to strictly protect its CIS systems against numerous outside and internal risks and vulnerabilities. Employees and students are important and critical players in protecting these district assets and in lessening the risks that can destroy these important and critical assets. Consequently, all individuals are required to fully comply with this policy, and to immediately report any violations or suspicious activities to the Superintendent or designee. Conduct otherwise will result in consequences described in this policy, and may be reported to appropriate authorities.</p>
-------------------	--

<p>2. Definitions 20 U.S.C. Sec. 6777</p> <p>18 U.S.C. Sec. 2256</p> <p>18 Pa. C.S.A. Sec. 6312</p> <p>Pol. 237</p>	<p>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 network that has access to the Internet, whether by wire, wireless, cable, or any other means.</p> <p>Child Pornography - under federal law, 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:</p> <ol style="list-style-type: none"> 1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. 2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that 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. <p>Under Pennsylvania law, any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.</p> <p>Computer - includes any district owned, leased or licensed or user-owned personal hardware, software, or other technology used on district premises or at district events, or connected to the district network, containing district programs or school district or student data including images, files, and other information attached or connected to, installed in, or otherwise used in connection with a computer.</p> <p>Computer includes, but is not limited to: desktop, notebook, powerbook, tablet PC or laptop computers, printers, cables, modems, and other peripherals including thumb and flash drives, 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 and/or camera/video and other capabilities, mobile phones or wireless devices, two-way radios/telephones, beepers, paging devices, laser pointers and attachments, and any other such technology developed.</p> <p>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</p>
---	---

	<p>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, photo optical 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, Global Positioning Systems, Personal Digital Assistants, facsimile machines, cell phones with or without Internet access and/or electronic mail and/or recording devices, cameras/video, and other capabilities.</p> <p>20 U.S.C. Sec. 6801 Educational Purpose - includes use of the CIS systems for classroom activities, professional or career development, and to support the district’s curriculum, policy and mission statement.</p> <p>47 U.S.C. Sec. 254 Harmful to Minors - under federal law, any picture, image, graphic image file or other visual depictions that:</p> <ol style="list-style-type: none"> 1. In 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 minors, an actual or simulated sexual act or sexual content, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals. 3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value as to minors. <p>18 Pa. C.S.A. Sec. 5903 Under Pennsylvania law, any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:</p> <ol style="list-style-type: none"> 1. Predominantly appeals to the prurient, shameful, or morbid interest of minors. 2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors. 3. Taken as a whole, lacks serious literary, artistic, political, educational or scientific value for minors. <p>Incidental personal use - incidental personal use of school computers is permitted for employees so long as such use does not interfere with the employee’s job duties and performance, with system operations, or with other system users. Personal use</p>
--	--

<p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p>must comply with this policy and all other applicable district policies, procedures and rules contained in this policy, as well as Internet service provider (“ISP”) terms, local, state and federal laws and must not damage the district’s CIS systems.</p> <p>Minor - for purposes of compliance with the Children’s Internet Protection Act (“CIPA”), an individual who has not yet attained the age of seventeen (17). For other purposes, minor shall mean the age of minority as defined in the relevant law.</p> <p>Network - a system that links two (2) or more computer systems, including all components necessary to effect the operation, including, but not limited to: computers, copper and fiber cabling, wireless communications and links, equipment closets and enclosures, network electronics, telephone lines, printers and other peripherals including thumb and flash drives, storage media, software, and other computers and/or networks to which the network may be connected, such as the Internet or those of other institutions.</p>
<p>18 U.S.C. Sec. 1460</p>	<p>Obscene - under federal law, analysis of the material meets the following elements:</p> <ol style="list-style-type: none"> 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, educational, or scientific value.
<p>18 Pa. C.S.A. Sec. 5903</p>	<p>Under Pennsylvania law, analysis of the material meets the following elements:</p> <ol style="list-style-type: none"> 1. The average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest. 2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene. 3. The subject matter, taken as a whole lacks serious literary, artistic, political, educational or scientific value.
<p>18 U.S.C. Sec. 2246 18 Pa. C.S.A. Sec. 5903</p>	<p>Sexual Act and Sexual Contact - as defined at 18 U.S.C. Sec. 2246, and at 18 Pa. C.S.A. Sec. 5903.</p>

<p>20 U.S.C. Sec. 6801 47 U.S.C. Sec. 254</p>	<p>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.</p>
<p>18 U.S.C. Sec. 1460, 2256</p>	<p>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.</p>
<p>3. Authority</p>	<p>Access to the district’s CIS systems through school resources is a privilege, not a right. These, as well as the user accounts and information, are the property of the school district. The district, further, reserves the right to deny access to prevent unauthorized, inappropriate or illegal activity or use, and may revoke those privileges and/or administer appropriate disciplinary action. The district will cooperate to the extent legally required with ISP, local, state and federal officials in any investigation concerning or related to the misuse of the CIS systems and/or violation of applicable laws or regulations.</p> <p>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. Employees and students have no privacy expectation in the contents of their personal files or any of their use of the school district’s CIS systems. The district reserves the right to monitor, track, log and access CIS systems use and to monitor and allocate files server space.</p>
<p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p>The district reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through general policy, software blocking or online server blocking. Specifically, the district operates and enforces technology protection measure(s) that block or filter 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, but is not limited to visual, graphic, text and any other form of obscene, sexually explicit, child pornographic, or other material that is harmful to minors, or that are hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, harassing, discriminatory as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability; violent, bullying, terroristic, and advocates the destruction of property. Measures designed to restrict adults’ and minors’ access to material harmful to minors may be disabled to enable an adult or student to access bona fide research, not within the prohibitions of this policy, or for another lawful purpose. No person may have access to material that is illegal under federal or state law.</p>

Expedited review and resolution of a claim that the policy is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee upon the receipt of a written consent from a parent/guardian for a student, and upon the written request from an employee.

The district has the right, but not the duty, to monitor, track, log, access and report all aspects of its computer information, technology and related systems of all users and of any user's personal computers, network, Internet, electronic communication systems, and media brought on to district premises or at district events, connected to the district network, containing school district programs or school district or student data including images, files, and other information, pursuant to the law, to ensure compliance with this policy and other district policies, to protect the district's resources, and to comply with the law.

Where the CIS system of the district has been used for illegal activity by either an employee and/or a student, the district shall report and turn over all relevant material to the appropriate authorities.

The district reserves the right to restrict or limit usage of lower priority CIS 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 student.
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 and local, state or federal law.

The district additionally reserves the right to:

1. Determine which CIS systems services will be provided through 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.

<p>5. Guidelines</p>	<p>7. Do not order any materials or use credit cards while using the school district's computers.</p> <p>8. 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 status.</p> <p>The Superintendent and/or designee will serve as the coordinator to oversee the school district's CIS systems and will work with other regional or state organizations as necessary, to educate employees, approve activities, provide leadership for proper training for all users in the use of the CIS systems and the requirements of this policy, establish a system to insure adequate supervision of the CIS systems, maintain executed user agreements, and interpret and enforce this policy.</p> <p>The Superintendent and/or designee 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.</p> <p>Unless otherwise denied for cause, student access to the CIS 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 the resources. All users have the responsibility to respect the rights of all other users within the school district and school district CIS systems, and to abide by the rules established by the district, its ISP, local, state and federal laws.</p> <p><u>Access To The CIS Systems</u></p> <p>CIS systems user accounts will be used only by authorized owners of the accounts for authorized purposes.</p> <p>An account will be made available according to a procedure developed by appropriate school district authorities.</p> <p>This policy, as well as other relevant district policies, will govern use of the district's CIS systems for users. Users' use of the CIS systems will also be governed by other relevant district policies.</p> <p>Types of services include, but are not limited to:</p> <ol style="list-style-type: none">1. World Wide Web - School district employees and students will have access to the Web through the school district's CIS systems as needed.
----------------------	--

2. E-Mail - School district employees may be provided assigned individual e-mail accounts for work related use, as needed. Students may be assigned individual e-mail accounts, as necessary, by the Director of Technology and/or designee at the recommendation of the teacher who will also supervise the students' use of the e-mail service.
3. Accounts - Independent contractors' consultants may receive an individual account with the approval of the Superintendent and/or designee if there is a specific, district-related purpose requiring such access. Use of the CIS systems by an independent contractor and/or consultant must be specifically limited to the district-related purpose.

Access to all data on, taken from, or compiled using school district computers is subject to inspection and discipline. Users have no right to expect that school district information placed on users' personal computers, networks, Internet, and electronic communications systems is beyond the access of the school district. The district reserves the right to legally access students' and employees' personal equipment for district information.

Parental Notification And Responsibility

The district will notify the parents/guardians about the district's CIS 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 wide range of social values in student use of the Internet. Further, the school district recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children. The district will encourage parents/guardians to specify to their children what material is and is not acceptable for their children to access through the district's CIS system.

School District Limitation Of Liability

The district makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the district's CIS systems will be error-free or without defect. The district does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the school district. The district is neither responsible for nor guarantees the accuracy or quality of the information obtained through or stored on the CIS systems. The district shall not be responsible for any damage users may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using the computers, network and

<p>Pol. 237</p>	<p>electronic communications systems. The district shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The district shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the district’s CIS 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 CIS systems.</p> <p><u>Prohibitions</u></p> <p>The use of the district’s CIS systems for illegal, inappropriate, unacceptable, or unethical purposes by users is prohibited. Such activities engaged in by users are strictly prohibited. The district reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the CIS systems.</p> <p>These prohibitions are in effect any time district resources are accessed whether on district property, when using mobile commuting equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when an employee or student uses their own equipment or when they publish a blog (web log). Students must also comply with the school district’s Electronic Devices policy.</p> <p><i>General Prohibitions</i></p> <p>Users are prohibited from using school district CIS systems to:</p> <ol style="list-style-type: none"> 1. Communicate about nonwork or nonschool-related communications unless the employees’ use comports with this policy’s definition of incidental personal use. 2. Send, receive, view, download, access or transmit material that is harmful to minors, indecent, obscene, pornographic, child pornographic, terroristic, or advocates the destruction of property. 3. Send, receive, view, download, access or transmit inappropriate matter and material likely to be offensive or objectionable to recipients including, but not limited to, that which may be defamatory; inaccurate; obscene; sexually explicit; lewd; hateful; harassing; discriminatory as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability; violent; vulgar; rude; inflammatory; threatening; profane; pornographic; offensive; terroristic and/or illegal. 4. Cyberbullying another individual.
-----------------	---

<p>Pol. 229, 610, 611, 612</p>	<ol style="list-style-type: none"> 5. Access or transmit gambling pools for money, including but not limited to, basketball and football, or any other betting or games of chance. 6. Participate in discussion or news groups that cover inappropriate and/or objectionable topics or materials, including those that conform to the definition of inappropriate matter in this policy. 7. Send terroristic threats, hateful mail, harassing communications, discriminatory remarks, and offensive, profane, or inflammatory communications. 8. Participate in unauthorized Internet Relay Chats, instant messaging communications and Internet voice communications (on-line; real-time conversations) that are not for school-related purposes or required for employees to perform their job duties. 9. Facilitate any illegal activity. 10. Communicate through e-mail for noneducational purposes or activities, unless it is for an incidental personal use as defined in this policy. The use of e-mail to mass mail noneducational or nonwork related information is expressly prohibited. For example, 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. 11. Engage in commercial, for-profit, or any business purposes, except where such activities are otherwise permitted or authorized under applicable district policies; conduct unauthorized fundraising or advertising on behalf of the district and nonschool organizations; resell district computer resources to individuals or organizations; or use the district's name in any unauthorized manner that would reflect negatively on the school district, its employees, or students. 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 district purchase of goods or supplies through the school district system. 12. Political lobbying. 13. Install, distribute, reproduce or use copyrighted software on district computers, or copy district software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright, as described in this policy.
------------------------------------	--

14. Install computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on district computers is restricted to the Superintendent or designee.
15. Encrypt messages using encryption software that is not authorized by the district from any access point on district equipment or district property. Employees and students must use district approved encryption to protect the confidentiality of sensitive or critical information in the district's approved manner.
16. Access, interfere, possess, or distribute confidential or private information without permission of the district's administration. An example includes accessing other students' accounts to obtain their grades.
17. Violate the privacy or security of electronic information.
18. Use the systems to send any district information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the district's business or educational interest.
19. Send unsolicited commercial electronic mail messages, also known as spam.
20. Post personal or professional web pages without administrative approval.
21. Post anonymous messages.

Access and Security Prohibitions

Users must immediately notify the Superintendent and/or designee if they have identified a possible security problem. Users must read, understand, provide a signed acknowledgement form(s), and comply with this policy that includes network, Internet usage, electronic communications, telecommunications, non-disclosure and physical information security policies. The following activities related to access to the district's CIS systems and information are prohibited:

1. Misrepresentation, including forgery, of the identity of a sender or source of communication.
2. Acquiring or attempting to acquire passwords of another. Users will be held responsible for the result of any misuse of users' names or passwords while the users' systems access were left unattended and accessible to others, whether intentional or through negligence.

3. Using or attempting to use computer accounts of others; these actions are illegal, even with consent, or if only for the purpose of browsing.
4. Altering a communication originally received from another person or computer with the intent to deceive.
5. Using district resources to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons, including, but not limited to, arranging for a drug sale or the purchase of alcohol, engaging in criminal activity, or being involved in a terroristic threat against any person or property.
6. Disabling or circumventing any district security, program or device, for example, but not limited to, anti-spyware, anti-spam software, and virus protection software or procedures.
7. Transmitting electronic communications anonymously or under an alias unless authorized by the school district.

Operational Prohibitions

The following operational activities and behaviors are prohibited:

1. Interference with or disruption of the CIS systems, network accounts, services or equipment of others, including, but not limited to, the propagation of computer “worms” and “viruses”, Trojan Horse and trapdoor program code, the sending of electronic chain mail, distasteful jokes, and the inappropriate sending of “broadcast” messages to large numbers of individuals or hosts. The user may not hack or crack the network or others’ computers, whether by parasiteware or spyware designed to steal information, or viruses and worms or other hardware or software designed to damage the CIS systems, or any component of the network, or strip or harvest information, or completely take over a person’s computer, or to “look around.”
2. Altering or attempting to alter files, system security software or the systems without authorization.
3. Unauthorized scanning of the CIS systems for security vulnerabilities.
4. Attempting to alter any school district computing or networking components including, but not limited to file servers, 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, whether wired, wireless, cable, or by other means.
6. Connecting unauthorized hardware and devices to the CIS systems.
7. Loading, downloading, or use of unauthorized games, programs, files, or other electronic media, including, but not limited to, downloading music files.
8. Intentionally damaging or destroying the integrity of the school district's electronic information.
9. Intentionally destroying the school district's computer hardware or software.
10. Intentionally disrupting the use of the CIS systems.
11. Damaging the school district's CIS systems networking equipment through the users' negligence or deliberate act.
12. Failing to comply with requests from appropriate teachers or school district administrators to discontinue activities that threaten the operation or integrity of the CIS systems.

Content Guidelines

Information electronically published on the school district's CIS systems shall be subject to the following guidelines:

1. Published documents including but not limited to audio and video clips or conferences, may not include a child's phone number, street address, or box number, name, other than first name, or the names of other family members without parental consent in writing.
2. Documents, web pages, electronic communications, or videoconferences may not include personally identifiable information that indicates the physical location of a student at a given time without parental consent in writing.
3. Documents, web pages, electronic communications, or videoconferences may not contain objectionable materials or point directly or indirectly to objectionable materials.

<p>Pol. 814</p>	<p>agreements. Employees will instruct students to respect copyrights, request permission when appropriate, and comply with license agreements and employees will respect and comply as well.</p> <p>Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing the law. The district does not permit illegal acts pertaining to the copyright law. Therefore, any user violating the copyright law does so at their own risk and assumes all liability.</p> <p>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; and deep-linking and framing into the content of others' web sites. Further, the illegal installation of copyrighted software or files for use on the district's computers is expressly prohibited. This includes all forms of licensed software, shrink-wrap, clickwrap, browwrap, and electronic software, downloaded from the Internet.</p> <p>School district guidelines on plagiarism will govern use of material accessed through the district's CIS systems. Users will not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices.</p> <p><u>Selection Of Material</u></p> <p>Board policies on the selection of materials will govern use of the district's CIS systems.</p> <p>When using the Internet for class activities, teachers shall select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers must 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 shall provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers shall 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.</p>
-----------------	---

relevant district policies, such as, but not limited to, the student and professional employee discipline policies, copyright policy, property policy, curriculum policies, terroristic threat policy, and harassment policies.

The user is responsible for damages to the 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 school district, appropriate legal authorities, whether the ISP, local, state, or federal law enforcement. The district will cooperate to the extent legally required with authorities in all such investigations.

Vandalism will result in cancellation of access to the district's CIS systems and resources and is subject to discipline.

Any and all costs incurred by the district for repairs and/or replacement of software, hardware and data files and for technological consultant services due to any violation of this policy, or federal, state, or local law, shall be paid by the user who caused the loss.

References:

PA Consolidated Statutes Annotated – 18 Pa. C.S.A. Sec. 5903, 6312

Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.

State Board of Education Regulations – 22 PA Code Sec. 403.1

U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq.

United States Code – 18 U.S.C. Sec. 1460, 2246, 2256,

20 U.S.C. Sec. 6801

Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777

Internet Safety – 47 U.S.C. Sec. 254

Board Policy – 105, 105.1, 105.2, 109, 218, 218.2, 229, 233, 237, 248, 317, 348, 610, 611, 612, 814