NORTHEASTERN EDUCATIONAL INTERMEDIATE UNIT 19

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF TECHNOLOGY RESOURCES

ADOPTED: June 26, 2012

REVISED:

815. ACCEPTABLE USE OF TECHNOLOGY RESOURCES

1. Purpose

Northeastern Educational Intermediate Unit provides employees, students and other authorized users with access to the Intermediate Unit's electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means.

Technology resources, including but not limited to, computers, network, Internet, electronic communications and information systems provide vast, diverse and unique capabilities. The Board shall provide access to the Intermediate Unit's technology resources in order to access information, research, to facilitate learning and teaching, and to foster the educational purpose and mission of the Intermediate Unit.

For users, the Intermediate Unit's technology resources must be used primarily for education related purposes and performance of Intermediate Unit job duties. Incidental personal use of 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 must comply with this policy and all other applicable Intermediate Unit 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 Intermediate Unit's technology resources. At the same time, personal technology devices brought onto the Intermediate Unit's property or suspected to contain Intermediate Unit information may be legally accessed to ensure compliance with this policy and other Intermediate Unit policies to protect the Intermediate Unit's resources, and to comply with the law.

The Intermediate Unit intends to strictly protect its technology resources against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting the Intermediate Unit's assets and in lessening the risks that can destroy these important and critical assets. Consequently, employees, students and other authorized users are required to fully comply with this policy, and to immediately report any violations or suspicious activities to the appropriate personnel. Violations of this policy shall result in actions further described in this policy and provided in other relevant Intermediate Unit policies.

	Due to the frequent changes in technology, additional rules and restrictions may be modified or added to this policy at any time.
2. Definitions	**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. The term child pornography is defined under both federal and state law.
18 U.S.C. Sec. 2256	**Child pornography** - under federal law, is 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 a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or 3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
18 Pa. C.S.A. Sec. 6312	**Child pornography** - under state law, is 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. **Computer** - includes any Intermediate Unit-owned, leased or licensed or user-owned personal hardware, software or other technology used on Intermediate Unit premises or at Intermediate Unit events, or connected to the Intermediate Unit network, containing Intermediate Unit programs or Intermediate Unit data (including images, files and other information) attached or connected to, installed in, or otherwise used in connection with a computer. Computer includes, but is not limited to: desktop, notebook, powerbook, tablet PC or laptop computers, printers, cables, modems and other peripherals; specialized electronic equipment used for students' special educational purposes; Global Position Systems (GPS) equipment; Personal Digital Assistants (PDAs) and handheld computers, iPads and iPods; cell phones, with or without Internet access and/or recording and/or camera and other capabilities, mobile phones or wireless devices; beepers; paging devices and two-way radios/telephones; laser pointers and attachments; 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, photo optical or photo electronic 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; PDA's; facsimile machines; cell phones with or without Internet access and/or electronic mail and/or recording devices; cameras; and other capabilities. The term harmful to minors is defined under both federal and state law.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	**Harmful to minors** - under federal law, is any picture, image, graphic image file or other visual depiction that: 1. Taken as a whole, with respect to minors, appeals to a 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 contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and 3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.
18 Pa. C.S.A. Sec. 5903	**Harmful to minors** - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it: 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; and 3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.

	Incidental Personal Use - use of Intermediate Unit technology resources by an individual employee for occasional, personal communications. Personal use must comply with this policy and all other applicable policies, procedures and rules, as well as ISP, local, state and federal laws, 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 Intermediate Unit reserves the right to monitor, track, access and log the use of its technology resources at any time.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	**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. **Network** - a system that links two (2) or more electronic technology devices, 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, Internet2, PAIUNet, or those of other institutions.
18 Pa. C.S.A. Sec. 5903	**Obscene** - any material or performance if: 1. The average person, applying contemporary community standards, would find that the subject matter, 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; and 3. The subject matter taken as a whole lacks serious literary, artistic, political, educational or scientific value.
18 U.S.C. Sec. 2246 18 Pa. C.S.A. Sec. 5903	**Sexual Act and Sexual Contact** - as defined at 18 U.S.C. § 2246(2) and at 18 U.S.C. § 2246(3) and 18 Pa. C.S.A. § 5903.
20 U.S.C. Sec. 9134 47 U.S.C. Sec. 254	**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.

3. Authority Pol. 218, 233, 317	Access to the Intermediate Unit's technology resources is a privilege, not a right. Technology resources, as well as the user accounts and information, are the property of the Intermediate Unit, which reserves the right to deny access to prevent further unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The Intermediate Unit will cooperate to the extent legally required with the ISP, local, state and federal officials in any investigation concerning or related to the misuse of technology resources. 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, the stored communication of user accounts for any reason in order to uphold this policy and to maintain the system. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the Intermediate Unit's technology resources, including personal files or any use of the Intermediate Unit's technology resources. The Intermediate Unit reserves the right to monitor, track, log and access technology resources and to monitor and allocate fileserver space.
24 P.S. Sec. 4604 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 Pol. 103, 103.1, 104, 218.2, 248, 249, 348	The Intermediate Unit reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the Intermediate Unit 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, 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, hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, harassing, discriminatory, violent, bullying, terroristic and advocates the destruction of property.
24 P.S. Sec. 4604	Upon request by students or staff, the Executive Director or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.
24 P.S. Sec. 4610 20 U.S.C. Sec. 6777	Upon request by students or staff, building administrators or program supervisors may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Executive Director or designee for expedited review.

	The Intermediate Unit 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 personal computers, network, Internet, electronic communication systems and media brought onto Intermediate Unit premises or at Intermediate Unit events, connected to the Intermediate Unit network, containing Intermediate Unit programs or Intermediate Unit or student data (including images, files and other information) to ensure compliance with this policy and other policies, to protect the Intermediate Unit's resources and to comply with law. The Intermediate Unit additionally reserves the right to: 1. Determine which technology resources services will be provided through Intermediate Unit 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. 4. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and any other applicable policies occurs or state or federal law is violated, including but not limited to those governing network use, copyright, security, privacy, employment and destruction of Intermediate Unit resources and equipment.
47 U.S.C. Sec. 254	The Board shall establish a list of materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors.
4. Delegation of Responsibility	The Intermediate Unit shall make every effort to ensure that technology resources are used responsibly by students and staff.
24 P.S. Sec. 4604	The Intermediate Unit shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the Intermediate Unit website, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request. Users of Intermediate Unit technology resources or Intermediate Unit-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the Intermediate Unit uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment.

Student user agreements shall also be signed by a parent/guardian.

Building administrators and program supervisors shall make initial determinations of whether inappropriate use has occurred.

20 U.S.C. Sec. 6777
47 U.S.C. Sec. 254
47 CFR Sec. 54.520

The Executive Director or designee shall be responsible for recommending technology and developing procedures used to determine whether the Intermediate Unit's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:

1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board.

2. Maintaining and securing a usage log.

3. Monitoring online activities of minors.

Employees must become proficient in the use of the Intermediate Unit's technology resources and software relevant to the employee's responsibilities and practice proper etiquette, ethical behavior, and agree to the requirements of this policy.

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

1. Be polite. Do not become abrasive in messages to others. General Intermediate Unit rules and policies for behavior and communicating apply.

2. Use appropriate language. Do not swear or use vulgarities or other inappropriate language.

3. Do not reveal the personal addresses or telephone numbers of others.

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

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

6. Consider all communications and information accessible via the Internet to be the property of the Intermediate Unit.

	7. Do not order any materials or use credit cards while using the Intermediate Unit's computers. 8. Respect the rights of other users
5. Guidelines	<u>Access To The Technology Resources</u> User accounts will be used only by authorized owners of the accounts for authorized purposes. An account will be made available according to a procedure developed by appropriate Intermediate Unit authorities.
Pol. 237	The Intermediate Unit's Acceptable Use of Technology Resources Policy will govern all use of the Intermediate Unit's technology resources. Student and staff use of technology resources will also be governed by other relevant policies. Types of services include, but are not limited to: 1. World Wide Web - Intermediate Unit employees, students, consortium members and guests will have access to the web through the Intermediate Unit's technology resources, as needed. 2. Internet2 - Intermediate Unit employees, students, consortium members and guests will have access to Internet2 through the Intermediate Unit's technology resources, as needed. 3. PAIUnet - Intermediate Unit employees, students, consortium members and guests will have access to PAIUnet through the Intermediate Unit's technology resources, as needed. 4. E-Mail - Intermediate Unit employees will be provided assigned individual e-mail accounts for work-related and incidental personal use, as needed. 5. Instant Messaging - Intermediate Unit employees may have access to local Instant Messaging within the Intermediate Unit local area network. 6. Video and Voice Conferencing - Intermediate Unit employees may have access to video and voice conferencing at their desktop.

7. Guest Access - Guests, which include but are not limited to visitors, workshop attendees, volunteers, independent contractors and adult education instructors, will have access to necessary technology resources of the Intermediate Unit. Use of these resources by a guest must be specifically limited to the Intermediate Unit-related purpose.

Educational Component

47 U.S.C. Sec. 254

Classroom teachers employed by the Intermediate Unit shall be responsible for providing instruction to their students who have access to the Internet and for monitoring their students when they are using the Internet. This instruction must include the following elements:

1. Educating minors about appropriate online behavior.

2. Interacting with other individuals on social networking websites and in chat rooms.

SC 1303.1-A
Pol. 249

3. Cyberbullying awareness and response.

4. Identifying themselves or providing identifying information to strangers online.

5. Public nature of materials posted online and the permanence of information posted online.

6. Online safety measures.

Teachers may contact the Technology Department for further direction and to obtain access to resource materials to assist in providing this training.

Limitation Of Liability

The Intermediate Unit makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the Intermediate Unit's technology resources will be error-free or without defect. The Intermediate Unit does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the Intermediate Unit, nor is the Intermediate Unit responsible for the accuracy or quality of the information obtained through or stored on the technology resources. The Intermediate Unit 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 electronic communications systems. The Intermediate Unit will not be responsible for stolen,

damaged or lost personal devices of employees, contractors and guests. The Intermediate Unit shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The Intermediate Unit shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the Intermediate Unit's technology resources. In no event shall the Intermediate Unit be liable to the user for any damages whether direct, indirect, special or consequential, arising out of the use of the technology resources.

Prohibitions

The use of the Intermediate Unit's technology resources for illegal, inappropriate, unacceptable, or unethical purposes by users is prohibited. Such activities engaged in by users are strictly prohibited and illustrated in this policy. The Intermediate Unit reserves the right to determine if any activity not stated in this policy constitutes an acceptable or unacceptable use of technology resources.

These prohibitions are in effect any time Intermediate Unit resources are accessed whether on Intermediate Unit 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, student or guest uses their own equipment.

General Prohibitions –

Users are prohibited from using Intermediate Unit technology resources to:

1. Communicate about nonwork or nonschool related communications unless the use complies with this policy's definition of incidental personal use.

2. Access or transmit material that is harmful to minors, indecent, obscene, pornographic, child pornographic, terroristic or advocates the destruction of property.

3. Access or transmit 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, violent, vulgar, rude, inflammatory, threatening, profane, pornographic, offensive, terroristic and/or illegal.

SC 1303.1-A
Pol. 249

4. Cyberbully another individual.

5. Access or transmit gambling or 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 which cover inappropriate and/or objectionable topics or materials, including those which conform to the definition of inappropriate matter in this policy.

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

8. 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.

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 business purposes (except where such activities are otherwise permitted or authorized under applicable Board policies); conduct unauthorized fundraising or advertising on behalf of the Intermediate Unit and nonschool organizations; resell Intermediate Unit computer resources to individuals or organizations not related to the Intermediate Unit; or use the Intermediate Unit's name in any unauthorized manner that would reflect negatively on the Intermediate Unit, its employees or students.

    Commercial purposes is defined as offering or providing goods or services or purchasing goods or services for personal use. Intermediate Unit acquisition policies will be followed for the purchase of goods or supplies through the Intermediate Unit system.

12. Political lobbying.

13. Install, distribute, reproduce or use copyrighted software on Intermediate Unit computers, or copy Intermediate Unit software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright.

14. Install computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on Intermediate Unit computers is restricted to the Technology Department.

15. Encrypt messages using encryption software that is not authorized by the Intermediate Unit from any access point on Intermediate Unit equipment or Intermediate Unit property. Employees must use Intermediate Unit approved encryption to protect the confidentiality of sensitive or critical information in the Intermediate Unit's approved manner.

16. Access, interfere, possess or distribute confidential or private information without permission of the Intermediate Unit 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 Intermediate Unit information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the Intermediate Unit'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 Technology Department if they have identified a possible security problem. The following activities related to access to the Intermediate Unit's technology resources 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. Users will be held responsible for the result of any misuse of the users' user name or password 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 purposes of "browsing".

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

5. Using Intermediate Unit resources to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons, such as arranging for the promotion of or the sale of drugs, alcohol or weapons; engaging in criminal activity; or being involved in a terroristic threat against any person or property.

6. Disabling or circumventing any Intermediate Unit 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 Intermediate Unit.

8. Intentionally encrypting communications for the sole purposes of avoiding security review.

Operational Prohibitions –

The following operational activities and behaviors are prohibited:

1. Interference with or disruption of the technology resources, 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, utilize spyware designed to steal information, or viruses and worms or other hardware or software designed to damage the technology resources, or any component of the network, or strip or harvest information, or completely take over a person's computer, or "looking around".

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

3. Unauthorized scanning of the technology resources for security vulnerabilities.

4. Attempting to alter any Intermediate Unit 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 retransmission 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 technology resources.

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 Intermediate Unit's electronic information.

9. Intentionally destroying the Intermediate Unit's computer hardware or software.

10. Intentionally disrupting the use of the technology resources.

11. Damaging the Intermediate Unit's technology resources/networking equipment through the users' negligence or deliberate act.

12. Failing to comply with requests from appropriate teachers or Intermediate Unit administrators to discontinue activities that threaten the operation or integrity of the technology resources.

13. Downloading and installing software from the Internet without authorization from the Technology Department.

<u>Content Guidelines</u>

Information electronically published on the Intermediate Unit's technology resources 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.
Pol. 814	4. Documents, web pages and electronic communications must conform to all Intermediate Unit policies and guidelines, including the copyright policy. 5. Documents to be published on the Internet must be edited and approved according to Intermediate Unit procedures before publication. <u>Purging E-Mail</u> Messages no longer needed for work-related purposes must be periodically purged by users from their personal electronic message storage areas. The Technology Department reserves the right to purge users' storage areas if storage space becomes critical. Technology Department will attempt to provide adequate notice before doing so. Users should be aware that this includes e-mail items stored in folders and subfolders. <u>Due Process</u> The Intermediate Unit will cooperate with the Intermediate Unit's ISP, local, state and federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through the Intermediate Unit's technology resources. Students or employees who possess due process rights for discipline resulting from the violation of this policy will be provided such rights. The Intermediate Unit may terminate the account privileges by providing notice to the user. <u>Search And Seizure</u> Violations of this policy, any other Intermediate Unit policy or the law may be discovered by routine maintenance and monitoring of the Intermediate Unit system, or any method stated in this policy, or pursuant to any legal means. The Intermediate Unit reserves the right to monitor, track, log and access any electronic communications, including, but not limited to, Internet access and e-mails at any time for any reason. Users should not have the expectation of privacy in their use of the Intermediate Unit's technology resources, and other Intermediate Unit technology, even when used for personal reasons.

	Everything that users place in their personal files should be written as if a third party will review it. <u>Copyright Infringement And Plagiarism</u> Federal laws, cases and guidelines pertaining to copyright will govern the use of material accessed through the Intermediate Unit resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing the law. The Intermediate Unit does not permit illegal acts pertaining to the copyright law. Therefore, any user violating the copyright law does so at his/her own risk and assumes all liability.
17 U.S.C. Sec. 101 et seq 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 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 Intermediate Unit's computers is expressly prohibited. Intermediate Unit guidelines on plagiarism will govern use of material accessed through the Intermediate Unit's technology resources. Users will not plagiarize works that they find. <u>Selection Of Material</u> The use of the technology resources shall be consistent with and enhance the curriculum adopted by the Intermediate Unit as well as the varied instructional needs, learning styles and abilities and developmental level of students. When using the Internet or private networks 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.

Employees have a professional responsibility to ensure responsible use of Intermediate Unit's technology resources by students and to help them develop the intellectual skills necessary to discriminate among information sources and evaluate the information for their educational goals.

District Systems

Intermediate Unit employees working in a district with access to district equipment and/or the district network must also comply with the district's Acceptable Use Policy. Users must comply with the acceptable use guidelines presented in this document and other documents for outside networks or services s/he may access through the Intermediate Unit and district electronic communication equipment.

Intermediate Unit Web Site

The Intermediate Unit will establish and maintain a web site and will develop and modify its web pages that will present information about the Intermediate Unit under the direction of the Technology Department. Publishers must comply with the Intermediate Unit's web site development procedures.

Safety And Privacy

To the extent legally required, users of the Intermediate Unit's technology resources will be protected from harassment or commercially unsolicited electronic communication. Any user who receives threatening or unwelcome communications must immediately take them to the Technology Department.

Users will not post personal contact information about themselves or other people on the technology resources. The user may not steal another's identity in any way, may not use spyware, cookies, or use Intermediate Unit or personel employee technology or resources in any way to invade one's privacy. Additionally, the user may not disclose, use or disseminate confidential and personal information (examples include, but are not limited to, using a cell phone with camera and Internet access to take pictures of anything, including, but not limited to, persons, places and documents relevant to the Intermediate Unit; saving, storing and sending the image with or without text or disclosing them by any means, including, but not limited to, print and electronic matter; social security numbers, home addresses, telephone numbers, school addresses, work addresses, credit card numbers, health and financial information, evaluations, psychological reports, educational records, reports and resumes or other information relevant to seeking the employment at the Intermediate Unit unless legitimately authorized to do so).

47 U.S.C. Sec. 254 47 CFR Sec. 54.520	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.
Pol. 218, 233, 317	<u>Consequences For Inappropriate, Unauthorized And Illegal Use</u> General rules for behavior, ethics and communications apply when using the technology resources and information, in addition to the stipulations of this policy. Users must be aware that violations of this policy or other policies, or for unlawful use of the technology resources, may result in loss of technology resource access and a variety of other disciplinary actions, including, but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, suspensions (with or without pay for employees), dismissal, expulsions and/or legal proceedings on a case-by-case basis. 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 Intermediate Unit, relevant school district(s), appropriate legal authorities, whether the ISP, local, state or federal law enforcement. The Intermediate Unit will cooperate to the extent legally required with authorities in all such investigations. Vandalism will result in cancellation of access to the Intermediate Unit's technology resources and is subject to discipline.

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

References:

School Code – 24 P.S. Sec. 1303.1-A

PA Crimes Code – 18 Pa. C.S.A. Sec. 5903, 6312

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

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

Sexual Abuse – 18 U.S.C. Sec. 2246

Sexual Exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256

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

Internet Safety, Children's Internet Protection Act – 47 U.S.C. Sec. 254

Children's Internet Protection Act Certifications, Title 47, Code of Federal Regulations – 47 CFR Sec. 54.520

Board Policy – 103, 103.1, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 814