MONTGOMERY COUNTY INTERMEDIATE UNIT #23

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEMS AND NETWORK

ADOPTED: May 26, 2004

REVISED: November 16, 2016

815. ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEMS AND NETWORK

1. Purpose

Montgomery County Intermediate Unit ("Intermediate Unit") provides employees, students and other authorized individuals with access to the Intermediate Unit's computers, 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 Intermediate Unit's networks and systems and to the Internet for staff members, internet consortium members and for students in order to access information, research, collaboration to facilitate learning and teaching, and to foster the educational purpose and mission of the Intermediate Unit.

Usage

For students and for staff, the Intermediate Unit's network and electronic communications systems are to be used primarily for education-related purposes and performance of MCIU 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 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.

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..

The term **child pornography** is defined under both federal and state law.

18 U.S.C. Sec. 2256(8)

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: 1. The production of such visual depiction involves the use of a minor engagingin 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.SA. Sec. 6312(d)	**Child pornography -** Under state 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. **Computer -** Includes any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with a computer. 20 U.S.C. § 6777(e)(1). Computer includes, but is not limited to: desktop, notebook, powerbook, tablet PC 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 Intermediate Unit's curriculum, policy and mission statement. 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(h)	**Harmful to Minors –** Under federal law, 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 minors, an actual or simulated sexual act or sexual content, 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(e)

Harmful to minors - Under state law, 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.

For purposes of this policy, any text or audio depictions of such matters shall be included in this definition.

Inappropriate Matter – Inappropriate matter includes, but is not limited to, visual, graphic, text and 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 (as it pertains to race, color, religion, national origin, gender, material status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, bullying, terroristic, and/or advocates the destruction of property.

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 their use is private. The Intermediate Unit reserves the right to monitor access and use of its network and electronic communications systems.

The Intermediate Unit Network - All components necessary to effect its 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, storage media, software, and other computers and/or networks to which the Intermediate Unit network may be connected, such as the Internet or those of other institutions.

Minor - For purposes of compliance with the Children's Internet Protection Act ("CIPA"), an individual who has not yet attained the age of seventeen. For other purposes, minor shall mean the age of minority as defined in the relevant law.

Network – A system that links two or more electronic devices, including all components necessary to effect the operation.

18 Pa. C.S.A. Sec. 5903

Obscene - Any material or performance that 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; and

3. Whether the work taken as a whole lacks serious literary, artistic, political, or scientific value.

Sexual Act and Sexual Contact - As defined at 18 U.S.C. Section 2246(2), and at 18 U.S.C. Section 2246(3), 18 Pa.C.S.A. Section 5903.

47 U.S.C. Sec. 254

Technology Protection Measure(s) (TPM) - A specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.

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.

Monitoring and Review; No Expectation of Privacy

3. Authority

Access to the Intermediate Unit's electronic communications systems and networks through Intermediate Unit 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 Intermediate Unit which reserves the right to deny access to prevent further unauthorized, inappropriate or illegal activity. In some instances Intermediate Unit employees and students use not only the Intermediate Unit network and electronic communications systems, but also the network and systems resources of a school or school district in which they are located. The employees and students must comply with both this policy and any policy that regulates their use of the network and systems in the school or school district in which they are

	using the network and systems. The Intermediate Unit will cooperate fully with schools, school districts, 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 Intermediate Unit's network or systems. The Intermediate Unit reserves the right, to monitor, track, log and access network and system use and to monitor and allocate fileserver space and other resources.
47 U.S.C. Sec. 254	The Intermediate Unit reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through software blocking or general policy. 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. 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.
47 U.S.C. Sec. 254	The Intermediate Unit reserves the right, but not the duty, to monitor, track, log, access and report all use of the Intermediate Unit's electronic communications systems and networks and Intermediate Unit electronic devices, as well as use by Intermediate Unit employees and students, of any personal electronic devices on Intermediate Unit premises or at Intermediate Unit events, connected to the Intermediate Unit network, and/or containing Intermediate Unit programs or data (including images, files, and other information), to the fullest extent permitted by law, to insure 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 further reserves the right, but not the duty, to monitor, track, log, access and report all use by Guest of personal electronic devices connected to the District network and/or containing Intermediate Unit programs or data, pursuant to the law, to insure 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 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 supports 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.

The Intermediate Unit additionally reserves the right to:

1. Determine which network and electronic communications systems services will be provided through Intermediate Unit resources.

2. View and monitor network traffic, file server 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. Notice will be provided to remove excess e-mail or files before being purged.

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 Intermediate Unit policies occurs or state or federal law is violated, including, but not limited to, those governing network use, copyright, security, discipline and vandalism of Intermediate Unit resources and equipment.

24 P.S.
Sec. 4604
20 U.S.C.
Sec. 6777
47 U.S.C.
Sec. 254

Due to the nature of the Internet as a global network connecting electronic devices around the world, inappropriate materials, including those which may be defamatory, inaccurate, obscene, lewd, vulgar, rude, harassing, violent, inflammatory, threatening, terroristic, hateful, bullying, 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 Intermediate Unit cannot completely block access to these resources. Accessing these and similar types of resources may be considered an unacceptable use of Intermediate Unit resources and will result in actions explained further in Section 12 Consequences for Inappropriate, Unauthorized and Illegal Use of this policy and as provided in relevant Intermediate Unit policies.

Users must become proficient in the use of the Intermediate Unit's network and electronic communications systems and software relevant to the use of the Intermediate Unit's network and electronic communications systems**;** practice proper etiquette and Intermediate Unit ethics; and agree to the requirements of this policy.

The Director of Technology Services and/or designee will serve as the coordinator to oversee the Intermediate Unit network and electronic communications systems and will work with other regional or state organizations as necessary.

4. Delegation of Responsibility	The Director of Technology Services and/or designee will approve activities, provide leadership for proper training of all staff in the use of the network and electronic communications systems and the requirements of this policy, establish a system to ensure adequate supervision of the network and electronic communications systems, maintain executed user agreements, and be responsible for interpreting this policy. The Director of Technology Services and/or designee will establish a process for for: setting up individual user, class and service accounts; setting quotas for resource allocation; establishing a retention schedule; and establishing the Intermediate Unit electronic device security/threat protection mechanisms. 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 Intermediate Unit and school district networks, electronic communications systems, and throughout the Internet, and to abide by the rules established by the Intermediate Unit, the internet consortium members, and their Internet Service Providers. The electronic information available to students and staff does not imply endorsement of the content by the Intermediate Unit, nor does the Intermediate Unit guarantee the accuracy of information received via the Internet. The Intermediate Unit 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 Intermediate Unit be responsible for material that is retrieved by the Internet, or the consequences that may result from them. The Intermediate Unit 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 Intermediate Unit be liable to the user for any damages whether direct, indirect, special or consequential, arising out the use of the Internet, network and electronic communications systems.
5. Guidelines	1. **<u>Access to the Network and Electronic Communications Systems</u>** a. Network and electronic communications systems user accounts will be used only by authorized owners of the accounts for authorized purposes. b. An account will be made available according to a procedure developed by appropriate Intermediate Unit authorities. c. **Intermediate Unit System**. The Intermediate Unit's Acceptable Use of the Electronic Communications Systems and Network Policy, as well as other relevant Intermediate Unit policies, will govern all use of the Intermediate Unit network and electronic communications systems. Student and staff use of the network and electronic communications systems will also be

governed by the other relevant Intermediate Unit policies, and where applicable, school or school district policies in which the computer, electronic communications system, or network is located.

d. Types of Services included, but not limited to:

i. **World Wide Web**- Intermediate Unit employees and students and consortium members will have access to the Web through the Intermediate Unit's networked computers and electronic communications systems as needed.

ii. **E-Mail**. Intermediate Unit employees and consortium members will be provided with an individual account as needed.

iii. **Guest Accounts**. Guests may receive an individual account with the approval of the Director of Technology Services and/or designee if there is a specific, Intermediate Unit-related purpose requiring such access. Use of the electronic communications system by a guest must be specifically limited to the Intermediate Unit-related purpose.

2. **Parental Notification and Responsibility**

The Intermediate Unit will notify the parents about the Intermediate Unit network and electronic communications systems and the policies governing their use through Intermediate Unit divisions. 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 Intermediate Unit to monitor and enforce a wide range of social values in student use of the Internet.

Further, the Intermediate Unit recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. The Intermediate Unit will encourage parents/guardians to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the Intermediate Unit's system. Parents/guardians are responsible for monitoring their children's use of the Intermediate Unit's networks when they are accessing the system from home.

3. **Intermediate Unit 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 network and communications systems will be error-free or without defect. The Intermediate Unit shall not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The Intermediate Unit is not responsible for the accuracy or quality of the information

obtained through or stored on the network and electronic communications systems. The Intermediate Unit shall not be responsible for financial obligations, charges or fees, arising through the unauthorized use of the Intermediate Unit's resources. In no event shall the Intermediate Unit be liable to the User for any damages whether direct, indirect, special or consequential, arising out the use of the network or electronic communications systems or electronic devices. To the contrary, should a User incur charges, such charges will be the User's responsibility.

4. **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. Such activities engaged in by all users are strictly prohibited and illustrated below. The Intermediate Unit 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 Intermediate Unit resources are accessed whether in school, directly from home, or indirectly through another Internet service provider.

a. 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 material that is harmful to minors, indecent, obscene, pornographic, child pornographic or terroristic.

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

24 P.S. 1303.1-A

4) Cyberbullying another individual.

5) Access or transmit gambling, pools for money, 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 (on-line; 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 non-educational purposes or activities, unless it is for an 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 distributions lists to offer personal items for sale is prohibited).

11) Commercial, for-profit, or business purposes (except where such activities are otherwise permitted or authorized under applicable Intermediate Unit policies), unauthorized fund raising or advertising on behalf of the Intermediate Unit and non-school Intermediate Unit organizations, reselling of Intermediate Unit computer resources to non-school Intermediate Unit individuals or organizations, or unauthorized use of the Intermediate Unit's name. 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 Intermediate Unit purchase of goods or supplies through the Intermediate Unit system.

12) Political lobbying except with the express approval of the Executive Director for Intermediate Unit job-related purposes.

13) Advertising of any kind, unauthorized fundraising or unauthorized use of the Intermediate Unit's name will not be permitted on the Internet or e-mail, or any other online service.

14) Anything that results in a copyright violation.

15) Install, distribute, reproduce or use of copyrighted software on Intermediate Unit computers, or the copying of Intermediate Unit software to unauthorized computer systems. The authority to install/download software on Intermediate Unit computers is restricted to Director of Technology Services, Assistant Director of Technology Services, Intermediate Unit Network staff and Intermediate Unit Technical Support staff.

16) Install computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on Intermediate Unit computers is restricted to Director of Technology Services, Assistant Director of Technology Services, Intermediate Unit Network staff and Intermediate Unit Technical Support staff.

17) Intentionally infringing upon the intellectual property rights of others.

18) Use of the network and electronic communications systems to commit plagiarism.

19) Making available material or information the possession or distribution of which is illegal.

20) Unauthorized access, interference, possession, or distribution of confidential or private information including reposing messages sent to them privately without permission of the person who sent the message.

21) Intentionally compromising the privacy or security of electronic information.

22) Using 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.

23) Sending unsolicited commercial electronic mail messages, also known as spam.

24) Posting personal and professional web pages without administrative approval.

b. <u>Access and Security Prohibitions</u>

Users must immediately notify the Director of Technology Services and/or designee if they have identified a possible security problem. The following activities related to access to the Intermediate Unit'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 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 a drug sale or the purchase of alcohol, engaging in criminal gang activity, being involved in a terroristic threat against any person or property.

7) Disabling or bypassing the Internet blocking/filtering software without authorization.

c. 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 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 or harvest 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 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 re- transmission of any computer, electronic communications systems, or network services, whether wire or wireless.

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 Intermediate Unit computer hardware or software.

10) Intentionally disrupting the use of electronic communications systems,

networks or information systems.

11) Negligence leading to damage of Intermediate Unit electronic information, computing, electronic communications systems, or networking equipment.

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

5. **Content Guidelines**

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

a. Published documents or video 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.

b. Documents, web pages, electronic communications, or video conferences 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.

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

d. Documents, web pages and electronic communications, must conform to Intermediate Unit policies and guidelines, including the copyright policy.

e. Documents to be published on the World Wide Web must be edited and approved according to Intermediate Unit procedures before publication.

6. **Due Process**

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

b. Disciplinary actions will be tailored to meet specific concerns related to the violation for staff, students and Internet consortium members. Student and staff violations will be handled in accordance with the

applicable provisions under local disciplinary codes.

c. The Intermediate Unit may terminate the account privileges by providing notice to the user.

7. **User's Consent to District Access and Disclosure**

a. User's 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. User consents to the Intermediate Unit's disclosure of information related to such violations as determined necessary by the Intermediate Unit to protect the Intermediate Unit's resources and to comply with the law.

b. The Intermediate Unit shall have the right, but not the obligation, to monitor, track, log, and access any electronic communications, including but not limited to, Internet access and e-mails. Students and employees should not have the expectation of privacy in electronic communications, even when used for personal reasons.

8. **Copyright Infringement and Plagiarism**

a. 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. Teachers will instruct students to respect copyright, request permission when appropriate, and comply with license agreements.

b. Violations of copyright law can be a felony and 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 Intermediate Unit's computers is expressly prohibited. This includes all forms of licensed software – shrink-wrap, clickwrap, browsewrap, and electronic software downloaded from the Internet. The Intermediate Unit 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.

c. Intermediate Unit guidelines on plagiarism will govern use of material accessed through the Intermediate Unit'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.

9. **Selection of Material**

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

b. 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.

10. **Intermediate Unit Web Site**

a. The Intermediate Unit will establish and maintain a Web Site and will develop Web pages that will present information about the Intermediate Unit under the direction of the Executive Director or designee.

11. **Safety & Privacy**

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

a. To the extent legally required, 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 the Director of Technology Services and/or designee.

b. 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 number, school address, and work address.

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

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

12. **Consequences for Inappropriate Use**

a. Failure to comply with this policy or inappropriate use of the Internet, Intermediate Unit network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings. Loss of Internet, electronic communications systems, and network access could be one of the disciplinary actions, however this policy incorporates all other relevant Intermediate Unit policies, such as, but not limited to, the student and professional employee discipline policies, copyright policy, property policy, curriculum policies, and sexual harassment.

b. 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 Intermediate Unit's resources.

24 P.S. 4604

c. 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.

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

e. Vandalism will result in cancellation of access to the Intermediate Unit's, and possibly the school district's, Internet, electronic communications systems and network resources and is subject to disciplinary action, and/or legal proceedings. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

	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 Exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256 Enhancing Education Through Technology Act – 20 U.S.C. Sec. 6777 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