Administrative Regulation

Acceptable Use of the Communications and Information Systems[1] 3515

Table of Contents



## 1.0 Purpose

The Central Susquehanna Intermediate Unit ("Intermediate Unit") provides employees, students, and Guests ("Users") with hardware, software, and access to the Intermediate Unit's Electronic Communication System and network, which includes Internet access, whether wired, wireless, cellular, virtual, cloud, or by any other means. Guests include, but are not limited to, visitors, workshop attendees, volunteers, adult education staff and students, board members, independent contractors, and Intermediate Unit consultants.

Computers, network, Internet, Electronic Communications, information systems, databases, files, software, and media, collectively called "CIS" systems, provide vast, diverse and unique resources. The Board of Directors will provide access to the Intermediate Unit's CIS systems for Users if there is a specific Intermediate Unit-related purpose to access information; to research and to collaborate; to facilitate learning and teaching; and/or to foster the Educational Purpose and mission of the Intermediate Unit.

[1] See Definitions section for the defined terms generally provided in initial capital letters throughout this Administrative Regulation and its accompanying Policy.

For Users, the Intermediate Unit's CIS systems must be used for Educational Purposes and performance of Intermediate Unit job duties in compliance with this Administrative Regulation and its accompanying Policy. Incidental Personal Use of Intermediate Unit Computers is permitted for employees as defined in this Administrative Regulation. However, they should have no expectation of privacy in anything they create, store, send, receive, or display on or over the Intermediate Unit's CIS systems, including their personal files, or any of their use. Students may only use the CIS systems for Educational Purposes.

CIS systems may include Intermediate Unit computers which are located or installed on Intermediate Unit property, at Intermediate Unit events, connected to the Intermediate Unit's network, or when using its mobile commuting equipment, telecommunication facilities in protected and unprotected areas or environments, directly from home, or indirectly through another internet service provider, and if relevant, when Users bring and use their own personal Computers or personal electronic devices, and, if relevant, when Users bring and use another entity's Computer or electronic device to an Intermediate Unit location, event, or connect it to the Intermediate Unit network.

If Users' bring personal Computers or personal electronic devices onto the Intermediate Unit property, to Intermediate Unit events, or connect them to the Intermediate Unit's network and systems, and if the Intermediate Unit reasonably believes the personal Computers and/or personal electronic devices contain Intermediate Unit information or contain information that violates a Intermediate Unit policy or administrative regulation, the legal rights of the Intermediate Unit or another person, or involves significant harm to the Intermediate Unit or another person, or involves a criminal activity, the personal Computers or personal electronic devices may be legally accessed *in accordance with the law* to ensure compliance with this Administrative Regulation, other Intermediate Unit policies, regulations, rules, procedures, ISP terms, and local, state, and federal laws. Users may not use their personal Computers and personal technology electronic devices to access the Intermediate Unit's intranet, Internet or any other CIS system unless approved by the Executive Director, and/or designee.

The Intermediate Unit intends to strictly protect its CIS systems against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting these Intermediate Unit assets and in lessening the risks that can destroy these important and critical assets. Consequently, Users are required to fully comply with this Administrative Regulation and its accompanying Policy, and to immediately report any violations or suspicious activities to the Security Officer/Telecommunications Manager, and/or designee. Conduct otherwise will result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section found in the last section of this Administrative Regulation, and provided in other relevant Intermediate Unit policies, regulations, rules, and procedures.

## 2.0 Definitions

**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 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. 20 U.S.C. § 6777; 18 U.S.C. § 2256(8); 47 U.S.C. § 254(h)(7)(F).

Under Pennsylvania law, any person who intentionally views or knowingly possesses or controls 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 is guilty of a felony of the third degree for their first offense, or guilty of a felony of the second degree for a second offense. 18 Pa.C.S.A. § 6312(d); 24 P.S. § 4603.

**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 or student 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, Intermediate Unit and Users: desktop, notebook, powerbook, tablet PC or laptop computers, servers, firewalls/security systems, distance learning equipment, videoconference units, printers, facsimile machine, cables, modems, and other peripherals; specialized electronic equipment used for students' special educational purposes; Global Positioning System (GPS) equipment; personal digital assistants (PDAs); iPods, MP3 players; USB/jump drives; iPads, Kindles, and other electronic readers; iPhones, cell phones, with or without Internet access and/or recording and/or camera/video and other capabilities and configurations, telephones, mobile phones, or wireless devices, two-way radios/telephones and other smartphones; beepers; paging devices, laser pointers and attachments, and any other such technology developed. 20 U.S.C. § 6777(e); 18 U.S.C. § 2256(6); Electronic Communications Device Policy and Administrative Regulation.

**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, without limitation, the Internet, intranet, electronic mail services, GPS, PDAs, facsimile machines, cell phones with or without Internet access and/or electronic mail and/or recording devices, cameras/video, and other capabilities and configurations.

**Educational Purpose** - Includes use of the CIS systems for classroom activities, professional or career development, and to support the Intermediate Unit's curriculum, policy and mission statement.

**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, educational or scientific value as to minors. 20 U.S.C. § 6777(e)(6); 47 U.S.C. § 254(h)(7)(G).

Under Pennsylvania 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; and

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. 18 Pa. C.S.A. § 5903(e)(6); 24 P.S. § 4603.

**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 must comply with this Administrative Regulation and all other applicable Intermediate Unit policies, administrative regulations, procedures and rules, as well as ISP terms, local, state and federal laws and must not damage the Intermediate Unit's CIS systems.

**Minor** – For purposes of compliance with the federal Children's Internet Protection Act ("FedCIPA"), 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. 47 U.S.C. § 254(h)(7)(D); 20 U.S.C. § 6777(e); 18 U.S.C. § 2256; 18 Pa.C.S.A. § 5903(e).

**Obscene** – Under Federal law, analysis of the material meets the following elements:

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

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

3. Whether the work taken as a whole lacks serious literary, artistic, political, educational, or scientific value. 18 U.S.C. § 1460; 20 U.S.C. § 6777(e); 47 U.S.C. § 254(h)(7)(E).

Under Pennsylvania law, any material or performance if:

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; and

3. The subject matter, taken as a whole lacks serious literary, artistic, political, educational or scientific value. 18 Pa.C.S.A. § 5903(b); 24 P.S. § 4603.

**Sexual Act and Sexual Contact** – As defined at 18 U.S.C. § 2246(2), and at 18 U.S.C. § 2246(3), 18 Pa.C.S.A. § 5903. 18 Pa.C.S.A. § 5903(e)(3);18 U.S.C. § 2246; 20 U.S.C. § 6777(e); 47 U.S.C. § 254(h)(7)(H).

**Technology Protection Measure(s)** – A specific technology that blocks or filters Internet access to Visual Depictions that are Obscene, Child Pornography or Harmful to Minors. 47 U.S.C. § 254(H)(&)(I); 24 P.S. § 4606.

**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. 18 Pa.C.S.A. § 2256; 18 U.S.C. § 1460(b).

## 3.0 Authority

Access to the Intermediate Unit'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 Intermediate Unit, which reserves the right to deny access to prevent 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 other educational entities, ISP, local, state and federal officials in any investigation concerning or related to the misuse of the CIS systems. 47 U.S.C. § 254(l); 24 P.S. § 510; 24 P.S. § 4604.

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 to access the stored communication of User accounts for any reason in order to uphold this Administrative Regulation, its accompanying Policy, other administrative regulations, the law, and to maintain the system. Users should have no privacy expectations in the contents of their personal files or any of their use of the Intermediate Unit's CIS systems. **USERS SHOULD HAVE NO EXPECTATION OF PRIVACY IN ANYTHING THEY CREATE, STORE, SEND, RECEIVE, OR DISPLAY ON OR OVER THE INTERMEDIATE UNIT'S CIS SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THE INTERMEDIATE UNIT'S CIS SYSTEMS. The Intermediate Unit reserves the right to record, check, receive, monitor, track, log access and otherwise inspect any or all CIS systems use and to monitor and allocate fileserver space. Users of the Intermediate Unit's CIS systems who transmit or receive communications and information shall be deemed to have consented to having the content of any such communication recorded, checked, received, monitored, tracked, logged, accessed and otherwise inspected or used by the Intermediate Unit, and to the monitoring and allocating fileserver space. Passwords and message delete functions do not restrict the Intermediate Unit's ability or right to access such communications or information.**

The Intermediate Unit 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 Intermediate Unit 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 as defined in this Administrative Regulation. Measures designed to restrict adults' and Minors' access to material Harmful to Minors may be disabled to enable an adult or a student (who has provided written consent from a parent or guardian) to access *bona fide* research, not within the prohibitions of this Administrative Regulation, or for another lawful purpose. No person may have access to material that is illegal under federal or state law. 20 U.S.C. § 6777(c); 24 P.S. § 4610.

Expedited review and resolution of a claim that this Administrative Regulation is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee, upon the receipt of written consent from a parent or guardian for a student, and upon the written request from an adult presented to the Executive Director or designee. 20 U.S.C. § 6777(c); 24 P.S. § 4610.

The Intermediate Unit has the right, but not the duty, to inspect, review, or retain Electronic Communication created, sent, displayed, received or stored on and over *the Intermediate Unit's* CIS systems and to monitor, record, check, track, log, access or otherwise inspect its CIS systems.

In addition, *in accordance with the law*, the Intermediate Unit has the right, but not the duty, to inspect, review, or retain Electronic Communications created sent, displayed, received, or stored *on User's* personal computers, electronic devices, networks, Internet, Electronic Communications Systems, and in databases, files, software, and media that contain Intermediate Unit information and/or data.

Also, *in accordance with the law*, the Intermediate Unit has the right, but not the duty, to inspect, review, or retain electronic communication created, sent, displayed, received or stored *on another entity's* computer or electronic device when Users bring and use another entity's computer or electronic device to a Intermediate Unit location, event, or connect it to the Intermediate Unit network and/or systems, and/or that contains Intermediate Unit programs, or Intermediate Unit data or information.

The above applies no matter where the use occurs whether brought onto Intermediate Unit property, to Intermediate Unit events, or connected to the Intermediate Unit network, or when using mobile commuting equipment and telecommunications facilities in protected or unprotected areas or environments, directly from home, or indirectly through another social media or internet service provider, as well as by other means. All actions must be conducted *in accordance with the law*, assist in the protection of the Intermediate Unit's resources, insure compliance with this Administrative Regulation, its accompanying Policy, or other Intermediate Unit policies, regulations, rules, and procedures, social media and internet service providers terms, or local, state, and federal laws.

The Intermediate Unit will cooperate to the extent legally required with social media sites, internet service providers, local, state, and federal officials in investigations or with other legal requests, whether criminal or civil actions.

The Intermediate Unit 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~~s~~ the education of the students.

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

3. Lowest – uses that include reasonable and limited educationally-related interpersonal communications and employee limited incidental personal use.
4. Forbidden – all activities in violation of this Administrative Regulation, other Intermediate Unit policies, regulations, rules, procedures, ISP terms, and local, state, or federal law.

The Intermediate Unit additionally reserves the right to:

1. Determine which CIS systems' services will be provided through Intermediate Unit resources.

2. Determine the types of files that may be stored on Intermediate Unit file servers and Computers.

3. 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, text messages, and other Electronic Communications.

4. Remove excess e-mail and other Electronic Communications or files taking up an inordinate amount of fileserver disk space after a reasonable time.

5. Revoke User privileges, remove User accounts, or refer to legal authorities, and/or Intermediate Unit authorities when violation of this or any other applicable Intermediate Unit administrative regulation, policy, rules, and procedures occurs or ISP terms, local, state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, social media, vendor access, data breach, and destruction of Intermediate Unit resources and equipment.

## 4.0 Responsibility

Due to the nature of the Internet as a global network connecting thousands of Computers around the world, Inappropriate Matter can be accessed through the network and electronic 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 the Consequences for Inappropriate, Unauthorized and Illegal Use section found in the last section of this Administrative Regulation, and as provided in relevant Intermediate Unit policies.

The Intermediate Unit must publish a current version of this Administrative Regulation and its accompanying Policy so that all Users are informed of their responsibilities. A copy of this Administrative Regulation, its accompanying Policy, and the *CIS Acknowledgement and Consent Form(s)* must be provided to all Users, who must sign the Intermediate Unit's Acknowledgement Form, either by electronic or written means.

Employees must be capable and able to use the Intermediate Unit's CIS systems and software relevant to the employee's responsibilities.

## 5.0 Delegation of Responsibility

The Security Officer/Telecommunications Manager, and/or designee, will serve as the coordinator to oversee the Intermediate Unit's CIS systems and will work with other regional or state organizations as necessary to educate Users, approve activities, provide leadership for proper training for all Users in the use of the CIS systems and the requirements of this Administrative Regulation and its accompanying Policy, establish a system to ensure adequate supervision of the CIS systems, maintain executed *User Acknowledgement and Consent Forms*, and interpret and enforce this Administrative Regulation.

The Security Officer/Telecommunications Manager, and/or designee, will establish a process for setting-up individual and class accounts, set quotas for disk usage on the system, establish Record Retention and Records Destruction Policies and a Records Retention Schedule to include electronically stored information (See Intermediate Unit Policy 3544), and establish the Intermediate Unit virus protection process.

Unless otherwise denied for cause, student access to the CIS systems resources must 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 Intermediate Unit and the Intermediate Unit CIS systems, and to abide by the rules established by the Intermediate Unit, the school district(s), its ISP, local, state and federal laws.

The Security Officer/Telecommunications Manager, and/or designee, has the responsibility to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. 47 U.S.C. § 254 (5)(B)(iii); 24 P.S. § 1303.1-A.

## 6.0 Guidelines

Access to the CIS Systems

The CIS systems accounts of Users must be used only by authorized owners of the accounts and only for authorized purposes.

An account will be made available according to a procedure developed by appropriate Intermediate Unit authorities.

The Intermediate Unit's Acceptable Use of Communications and Information Systems Policy, this Administrative Regulation, as well as other relevant Intermediate Unit policies, administrative regulations, rules, and procedures, will govern use of the Intermediate Unit's CIS systems for Users.

Types of Services include, but are not limited to:

1. Internet - Intermediate Unit employees, students, and Guests will have access to the Internet through the Intermediate Unit's CIS systems, as needed.

2. E-Mail and Text Messaging - Intermediate Unit employees may be assigned individual e-mail and text messaging accounts for work-related use, as needed. Students may be assigned individual e-mail accounts, as necessary, by the Security Officer/Telecommunications Manager and/or designee, and at the recommendation of the teacher who will also supervise the students' use of the e-mail service**.** Students and Guests may not be assigned text message accounts.

3. Guest Accounts - Guests may receive an individual Internet account with the approval of the Security Officer/Telecommunications Manager and/or designee if there is a specific Intermediate Unit related purpose requiring such access. Use of the CIS systems by a Guest must be specifically limited to the Intermediate Unit-related purpose and comply with this Administrative Regulation, and all other Intermediate Unit policies (including the Vendor Access Policy), procedures, and rules, as well as Internet Service Provider ("ISP") terms, local, state and federal laws and may not damage the Intermediate Unit's CIS systems. An Intermediate Unit *CIS Acknowledgement and Consent Form* must be signed, and if the Guest is a Minor, a parent's or legal guardian's written signature is required.

4. Blogs - Employees may be permitted to have Intermediate Unit-sponsored blogs, after they receive training, and the approval of the Security Officer/Telecommunications Manager, or designee. All bloggers must follow the rules provided in this Administrative Regulation, and all other applicable policies (for example, the Intermediate Unit's Acceptable Use Policy, and Social Media Policy), regulations (for example, the Intermediate Unit's Social Media Administrative Regulation), rules, and procedures of the Intermediate Unit, as well as ISP terms, and local, state, and federal laws.

5. Web 2.0 Second Generation and Web 3.0 Third Generation Web-based Services - Certain Intermediate Unit authorized Second Generation and Third Generation Web-based services, such as blogging, authorized social networking sites, wikis, podcasts, RSS feeds, social software, folksonomies and collaboration tools that emphasize online participatory learning (where Users share ideas, comment on one another's project, plan, design, or implement, advance or discuss practices, goals, and ideas together, co-create, collaborate and share) among Users may be permitted by the Intermediate Unit, however, such use must be approved by the Coordinator of Technology Services and/or designee, followed by training authorized by the Intermediate Unit. Users must comply with this Administrative Regulation, and its accompanying Policy, as well as any other relevant policies (including the Intermediate Unit's Social Media Policy), regulations (for example, the Intermediate Unit's Social Media Administrative Regulations) rules, and procedures including the copyright, ISP terms, and local, state, and federal laws during such use.

Parental Notification and Responsibility

The Intermediate Unit will notify the parents/guardians about the Intermediate Unit CIS systems and the policies, regulations, rules, and procedures governing their use. This Administrative Regulation 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 and guardians 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 School's District's CIS system. Parents/Guardians are responsible to help monitor their child(ren)'s use of the Intermediate Unit's CIS systems when they are accessing the systems.

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's CIS systems 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 CIS systems. 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 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 CIS 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 CIS systems.

Student Use of Electronic Communication Devices

The Board permits Silent Use of Electronic Communication Devices, including Personal Electronic Communication Devices, by Intermediate Unit students during the school day in Intermediate Unit buildings, on Intermediate Unit property, and while students are attending School-District-sponsored activities during regular school hours when they are in compliance with the student Electronic Communication Devices Administrative Regulation accompanying this Policy, other Intermediate Unit policies, regulations, rules, and procedures, and so long as such use does not interfere with the students' educational requirements, responsibilities/duties and performance, the rights and education of others, and the operation and services of the Intermediate Unit.

The Executive Director has been granted the authority to create, modify, update, and enforce a Student Electronic Communication Devices Administrative Regulation, and accompanying regulation(s), rules, procedures, and forms, if needed. See Electronic

Communication Devices Administrative Regulation 3515.2.

The Intermediate Unit strictly prohibits possession by students on school grounds, at Intermediate Unit-sponsored activities, and on buses or other vehicles provided by the Intermediate Unit any non-Intermediate Unit-owned laser pointers, or laser pointer attachments, and any Electronic Communication Devices, including Personal Electronic Communication Devices, that are hazardous or harmful to students, employees, and the Intermediate Unit. These include, but are not limited to, devices that control/interfere with the operation of the buildings' systems, facilities and infrastructure, or digital network. No exception or permission may be authorized by the supervisors and/or administrators, or designee, or anyone, for students to possess or use such devices.

Supervisors and administrators, in consultation with the Executive Director and in compliance with the Student Electronic Communication Devices Administrative Regulation, other Intermediate Unit policies, regulations, rules, and procedures, are authorized to determine the extent of the use of Electronic Communication Devices, including Personal Electronic Communication Devices, within their programs, classrooms, and schools, on the Intermediate Unit's property, and while students are attending that Intermediate Unit's sponsored activities during regular school hours. For example, use of Electronic Communication Devices, including Personal Electronic Communication Devices, at the elementary grade level may be different than that at the middle school, and/or high school grade levels.

Unless a teacher determines otherwise, Electronic Communication Devices, including Personal Electronic Communication Devices, must be turned off upon entering any instructional area and remain off until the student leaves the instructional area. Instructional areas include, but are not limited to, classrooms, gymnasiums, practice fields, field trip locations, auditoriums, band rooms, and chorus rooms.

Prohibitions

The use of the Intermediate Unit's CIS systems for illegal, inappropriate, unacceptable, or unethical purposes by Users is prohibited. Such activities engaged in by 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 CIS systems.

These prohibitions are in effect any time Intermediate Unit resources are accessed whether on Intermediate Unit property, at Intermediate Unit events, while connected to the Intermediate Unit's network, when using mobile commuting equipment, telecommunication facilities in protected and unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when an employee or student uses their own equipment.

*General Prohibitions –*

Users are prohibited from using Intermediate Unit CIS systems to:

1. Communicate about nonwork or non-school related matters unless the employees' use comports with the definition of Incidental Personal Use in this Administrative Regulation.

2. Send, receive, view, download, store, access, print, distribute, or transmit material that is Harmful to Minors, indecent, Obscene, pornographic, Child Pornographic, terroristic, sexually explicit, sexually suggestive. This includes but is not limited to, Visual Depictions. Examples include, taking, disseminating, transferring, or sharing Obscene, pornographic, lewd, or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (such as, sexting, e-mailing, texting, among others). Nor may Users advocate the destruction of property.

3. Send, receive, view, download, store, access, print, distribute, or transmit Inappropriate Matter as defined in this Administrative Regulation, and material likely to be offensive or objectionable to recipients.

4. Cyberbully another individual or entity. See Intermediate Unit's Bullying/Cyberbullying Policy. 24 P.S. §13-1301.1-A; Cyberbullying Policy 5144.1

5. Access or transmit gambling information or promote or participate in 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 Administrative Regulation.

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

8. Participate in unauthorized Internet Relay Chats 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. Students must obtain consent from their teacher to use IRCs, however, they may not use instant messaging or text messaging.

9. Use in an illegal manner or to facilitate any illegal activity.

10. Communicate through e-mail, instant messaging, or text messages for non-educational purposes or activities, unless it is for Incidental Personal Use as defined in this Administrative Regulation. The use of e-mail to mass mail non-educational or non-work related information is expressly prohibited (for example, the use of the "everyone distribution list, or all staff lists, building level distribution lists, or other e-mail distributions 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 Intermediate

Unit policies); conduct unauthorized fund raising or advertising on behalf of the Intermediate Unit and non-school Intermediate Unit organizations; engage in the resale of Intermediate Unit computer resources to individuals or organizations; 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 Intermediate Unit purchase of goods or supplies through the Intermediate Unit system.

12. Engaging in political lobbying or advocacy.

13. Install, distribute, reproduce or use unauthorized 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. See Section Copyright Infringement in this Administrative Regulation, the Intermediate Unit's Copyright Policy 3543 and Copyright Guidelines Handbook for additional information.

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 Security Officer/Telecommunications Manager, and/or designee.

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. Users 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's administration. An example includes accessing other students' accounts to obtain their grades, or accessing other employees' accounts to obtain information.

17. Violate the privacy or security of electronic information.

18. 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.

22. Use the name of the "Central Susquehanna Intermediate Unit" in any form in blogs on Intermediate Unit Internet pages or websites not owned or related to the Intermediate Unit, or in forums/discussion boards, and social media sites, to express or imply the position of the Central Susquehanna Intermediate Unit without the expressed, written permission of the Executive Director, and/or designee. When such permission is granted, the posting must state that the statement does not represent the position of the Intermediate Unit.

23. Bypass or attempt to bypass Internet filtering software by any method including, but not limited to, the use of anonymizers/proxies or any websites that mask the content the User is accessing or attempting to access.

24. Advocate illegal drug use, whether expressed or through a latent pro-drug message. This does not include a restriction of political or social commentary on issues, such as the wisdom of the war on drugs or medicinal use.

25. Attempt to or obtain personal information under false pretenses with the intent to defraud another person.

26. Use location devices to invade a person's privacy or to harm or put another person in jeopardy.

27. Plagiarize works that are found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.

28. Post false statements, or steal the identity of another person.

*Access and Security Prohibitions –*

Users must immediately notify the Security Officer/Telecommunications Manager, and/or designee, if they have identified a possible security problem. Users must read, understand, and submit a signed *CIS Acknowledgement and Consent Form(s),* and comply with this Administrative Regulation that includes network, Internet usage, Electronic Communications, telecommunications, non-disclosure and physical and information security requirements. The following activities related to access to the Intermediate Unit'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 User IDs and passwords of another. Users are required to use unique strong passwords that comply with the Intermediate Unit's password, authentication, and syntax requirements. Users will be held responsible for 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 Intermediate Unit resources to engage in any illegal act or any activity, which may threaten the health, safety or welfare of any person or persons. Such acts would include, but are not be limited to, arranging for a drug, engaging in criminal activity, or being involved in a terroristic threat against any person or property. Although not necessarily an illegal act, such prohibited activity would include arranging for the purchase of alcohol.

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. Accessing any website that the Intermediate Unit has filtered or blocked as unauthorized. Examples include, but are not limited to, unauthorized social media, music and video download, and gaming sites.

9. Installing or attaching keylogging devices, keylogging mechanisms, or keylogging software of any kind.

Users must protect and secure all electronic resources and information, data and records of the Intermediate Unit from theft and inadvertent disclosure to unauthorized individuals or entities at all times. If any User becomes aware of the release of Intermediate Unit information, data or records, the release must be reported to the Security Officer/Telecommunications Manager immediately. See the Intermediate Unit's Data Breach Notification Policy 3521 for further information.

*Operational Prohibitions –*

The following operational activities and behaviors are prohibited:

1. Interference with, infiltration into, 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 trapdoor, robot, spider, crawler, program code, the sending of electronic chain mail, distasteful jokes, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts. Users may not hack or crack the network or others' Computers, whether by malware or spyware designed to steal information, or viruses and worms or other hardware or software designed to damage the CIS systems, or the system of others, or any component of the network, or strip or

harvest information, or completely take over a person's Computer, or to "look around". See Policy 3521.

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 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 wired, wireless, cable, virtual, cloud, cellular, 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 is not limited to, downloading unauthorized music and video 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 CIS systems.

11. Damaging the Intermediate Unit's Computers, CIS systems, networking equipment through the Users' negligence or deliberate act, including but not limited to vandalism.

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

Content Guidelines

Information electronically published on the Intermediate Unit'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 student's date of birth, Social Security number, driver' license number, financial information, credit card number, health information, phone number(s), street address, or box number, name (other than

first name) or the names of other family members without parent or guardian consent.

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 parent or guardian consent.

3. Documents, web pages, Electronic Communications, or videoconferences may not contain objectionable materials or point directly or indirectly to objectionable materials.

4. Documents, web pages and Electronic Communications, must conform to all Intermediate Unit policies, administrative regulations, rules, and procedures.

5. Documents to be published on the Internet must be edited and approved according to Intermediate Unit policies, regulations, rules, and procedures before publication.

Due Process

The Intermediate Unit will cooperate with the Intermediate Unit's ISP's rules, 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 CIS systems.

If students or employees possess due process rights for discipline resulting from the violation of this Administrative Regulation and its accompanying Policy, they will be provided such rights.

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

Search and Seizure

Users' violations of this Administrative Regulation, its accompanying Policy, and any other Intermediate Unit policy, regulations, rules, or procedures, ISP terms, or the law may be discovered by routine maintenance and monitoring of the School District CIS system, or any method stated in this Administrative Regulation, or pursuant to any legal means.

The Intermediate Unit reserves the right, but not the duty, to inspect, review, or retain Electronic Communications created, sent, displayed, received, or stored on or over its CIS systems; to monitor, track, log, access, or otherwise inspect; and/or report all aspects of its CIS systems. This includes items related to any personal Computers, network, Internet, Electronic Communication Systems, databases, files, software, and media that individuals may bring onto the Intermediate Unit's property, or to Intermediate Unit events, that were connected to the Intermediate Unit's network, and/or that contain Intermediate Unit programs, or Intermediate Unit or Users' data and information, *in accordance with the law*, in order to insure compliance with this Administrative

Regulation, other Intermediate Unit policies, regulations, rules, and procedures ISP terms, and local, state, and federal laws to protect the Intermediate Unit's resources, and to comply with the law.

**USERS SHOULD HAVE NO EXPECTATION OF PRIVACY IN ANYTHING THEY CREATE, STORE, SEND, RECEIVE, OR DISPLAY ON OR OVER THE INTERMEDIATE UNIT'S CIS SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THE INTERMEDIATE UNIT'S CIS SYSTEMS. The Intermediate Unit reserves the right to record, check, receive, monitor, track, log access and otherwise inspect any or all CIS systems' use and to monitor and allocate fileserver space.**

Everything that Users place in their personal files should be entered with the knowledge and understanding that it is subject to review by a third party.

Copyright Infringement and Plagiarism

Federal laws, cases, policies, regulations, and guidelines pertaining to copyright will govern the use of material accessed through the Intermediate Unit resources. See Policy 3543. Users will make a standard practice of requesting permission from the holder of the work, or complying with the Fair Use Doctrine, and/or complying with license agreements. Employees will instruct Users to respect copyrights, request permission when appropriate, and to comply with the Fair Use Doctrine, and/or license agreements. Employees will respect and comply as well. 17 U.S.C. § 101 et seq.; Copyright Policy and Administrative Regulation 3543.

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 their own risk and assumes all liability.

Violations of copyright law include, but are not limited to, making unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over Computer networks, remixing or preparing mash-ups that violate the law, and 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.

No one may circumvent a Technology Protection Measure that controls access to a protected work unless they are permitted to do so by law. No one may manufacture, import, offer to the public, or otherwise traffic in any technology, product, service, device, component or part that is produced or marketed to circumvent a technology protection measure to control access to a copyright protected work. 17 U.S.C. § 1202; 17 U.S.C. § 1202.

Intermediate Unit guidance on plagiarism will govern use of material accessed through the Intermediate Unit's CIS systems. Users must not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices. Users understand that use of the Intermediate Unit's CIS systems may involve the Intermediate Unit's use of plagiarism analysis software being applied to their works.

Selection of Material

Intermediate Unit policies, administrative regulations, rules, and procedures on the selection of materials will govern use of the Intermediate Unit's CIS systems.

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 must preview the materials and websites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the website. Teachers must 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.

Intermediate Unit Website

The Intermediate Unit has established and maintains a Website and will develop and modify its web pages that will present information about the Intermediate Unit under the direction of the Security Officer/Telecommunications Manager, and/or designee. Publishers must comply with this Administrative Regulation, other Intermediate Unit policies, regulations, rules, procedures, ISP terms, and local, state, and federal laws.

The Intermediate Unit may limit its liability by complying with the Digital Millennium Copyright Act's safe harbor notice and takedown provisions. 17 U.S.C. § 512.

Blogging

If an employee, student or Guest creates a blog with their own resources and on their own time, the employee, student, or Guest may not violate the privacy rights of employees and students, may not use Intermediate Unit personal and private information/data, images, equipment, resources, and copyrighted material in their blog, and may not disrupt the Intermediate Unit. See also the Intermediate Unit's Social Media Policy 3515.1, and its accompanying administrative regulations.

Contrary conduct will result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section of this Administrative Regulation, and provided in relevant Intermediate Unit policies, regulations, rules, and procedures.

Safety and Privacy

To the extent legally required, Users of the Intermediate Unit's CIS systems will be protected from harassment or commercially unsolicited Electronic Communication. Any User who receives threatening or unwelcome communications is strong encouraged to immediately send or otherwise provide them to the Security Officer/Telecommunications Manager and/or designee.

Users must not post unauthorized personal contact information about themselves or other people on the CIS systems. Users may not steal another's identity in any way, may not use spyware, cookies, or other program code, keyloggers, and may not use Intermediate Unit or personal technology or resources in any way to invade another's privacy. Additionally, Users may not disclose, use or disseminate confidential and personal information about students or employees. Examples include, but are not limited to, revealing biometric data, student grades, Social Security numbers, dates of birth, 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 employment at the Intermediate Unit by using a PDA, iPhone, Blackberry, cell phone (with or without camera/video and Internet access), and to other Computers, unless legitimately authorized to do so. 47 U.S.C. §254.

If the Intermediate Unit requires that data and information be encrypted, Users must use Intermediate Unit authorized encryption to protect their security.

Student Users, by their use of the Intermediate Unit's CIS System, agree not to meet with someone they have met online unless they have parent or guardian consent.

Consequences for Inappropriate, Unauthorized and Illegal Use

General rules for behavior, ethics, and communications apply when using the CIS systems and information, in addition to the stipulations of this Administrative Regulation, its accompanying Policy, other Intermediate Unit policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws. Users must be aware that violations of this Administrative Regulation, its accompanying Policy, or other Intermediate Unit policies, regulations, rules, and procedures, or for unlawful use of the CIS systems, may result in loss of CIS 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, student suspensions, employee suspensions (with or without pay), dismissal, expulsions, breach of contract, and/or legal proceedings. This will be handled on a case-by-case basis. This Administrative Regulation incorporates all other relevant Intermediate Unit policies, such as, but not limited to, the student and professional employee discipline policies, Code of Student Conduct, acceptable use, copyright, social media, data breach, property, curriculum, terroristic threat, vendor access, student electronic device, and harassment policies.

The User is responsible for damages to Computers, the network, equipment, Electronic Communications Systems, and software resulting from accidental, negligent, deliberate, and willful acts. Users or, in the event the User is a minor, the parent or guardian will also be responsible for incidental or unintended damage resulting from negligent, willful or deliberate violations of this Administrative Regulation, its accompanying Policy, other Intermediate Unit related policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws. For example, Users will be responsible for payments related to lost or stolen Computers and/or Intermediate Unit equipment, and recovery and/or breach of the data contained on them.

Violations as described in this Administrative Regulation, its accompanying Policy, other Intermediate Unit policies, regulations, rules, and procedures may be reported to the Intermediate Unit, and to appropriate legal authorities, whether the ISP, local, state, or federal law enforcement. Actions that constitute a crime under state and/or federal law, could result in arrest, criminal prosecution, and/or lifetime inclusion on a sexual offenders registry. 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 CIS systems and 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 consultant services due to any violation of this Administrative Regulation, its accompanying Policy, other Intermediate Unit policies, regulations, rules, and procedures, or ISP terms, or federal, state, or local law, shall be paid by the User or, in the case of a minor User, the parent or guardian of the minor who caused the loss.

Reference**:** Board Policies, Administrative Regulations, Rules, and Procedures

Legal Authorization: PA Consolidated Statutes Annotated – 18 Pa. C.S.A. § 5903, 6312; PA; Child Internet Protection Act – 24 P.S. § 4601 et seq.; PA Bullying Act – 24 P.S. § 13-1303.1-A; PA – 18 Pa. C.S.A. § 6312; 24 P.S. § 4603, 4604; PA School Code – 24 P.S. § 9-908-A, 9-914-A U.S. Copyright Law – 17 U.S.C. § 101 et seq.; Digital Millennium Copyright Act 17 U.S.C. § 512, 1202; United States Code – 18 U.S.C. § 1460, 2246, 2252, 2256; 47 U.S.C. § 254; Enhancing Education Through Technology Act of 2001 – 20 U.S.C. § 6777; Federal Children's Internet Protection Act – 47 U.S.C. § 254

Adopted: June 20, 2012

Published: June 21, 2012