Policy

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

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 to collaborate; to facilitate learning and teaching; and/or to foster the Educational Purpose and mission of the Intermediate Unit.

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 Policy and its accompanying Administrative Regulation(s). Incidental Personal Use of Intermediate Unit Computers is permitted for employees as defined in the Administrative Regulation(s). 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

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

contain information that violates an 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, then the personal Computers or personal electronic devices may be legally accessed *in accordance with the law* to ensure compliance with this Policy, its accompanying Administrative Regulation(s), 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 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 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 Policy and its accompanying Administrative Regulation(s), 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 Policy and its accompanying Administrative Regulation(s), and provided in other relevant Intermediate Unit policies, regulations, rules, and procedures.

2.0 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 Policy and its accompanying Administrative Regulation(s), establish a system to insure adequate supervision of the CIS systems, maintain executed *User Acknowledgement and Consent Forms*, and interpret and enforce this Policy and its accompanying Administrative Regulation(s).

The Executive Director is granted the authority to create, modify, update, and enforce accompanying Administrative Regulation(s) to this Acceptable Use Policy. This Policy must be incorporated into its accompanying Administrative Regulation(s), and the Administrative Regulation(s) must include, without limitation: Purpose, Authority,

Responsibility, Delegation of Responsibility, and Guidelines that include, but are not limited to:

Access to the CIS Systems
Parental Notification and Responsibility
Intermediate Unit Limitation of Liability
Student Use of Electronic Communication Devices
Prohibitions
    General Prohibitions
    Access and Security Prohibitions
    Operational Prohibitions
Content Guidelines
Due Process
Copyright Infringement and Plagiarism
Selection of Material
Intermediate Unit Website
Blogging
Safety and Privacy
Consequences for Inappropriate, Unauthorized, and Illegal Use

3.0 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 Policy and its accompanying Administrative Regulation(s), other Intermediate Unit policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws. Users must be aware that violations of this Policy and its accompanying Administrative Regulation(s), 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 Policy and its accompanying Administrative Regulation(s) incorporate all other relevant Intermediate Unit policies, such as, but not limited to, the student and professional employee discipline policies, Code of Student Conduct, 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. User will also be responsible for incidental or unintended damage resulting from negligent, willful or deliberate violations of this Policy and its accompanying Administrative Regulation(s), other Intermediate Unit related policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws. For example, Users or, in the event the User is a minor, the parent or guardian 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 Policy and its accompanying Administrative Regulation(s), 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 Policy and its accompanying Administrative Regulation(s), 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; 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