CSIU Policy

Social Media Policy (Employees, Students, Guests) 3515.1

(1) Purpose

(1.1) Today, both Intermediate Unit educational social media and commercial social media exist for Users to utilize. Therefore, social media can be used either as part of the Intermediate Unit's educational mission or for business purposes, or as part of the Users personal commercial online presence. Mobile electronic devices, portable or stationary computers, and Intermediate Unit networks and systems, as well as Users' networks, systems, computers, and devices are available for (or provided for) Users to carry out their social media activities. The purpose of the Central Susquehanna Intermediate Unit ("Intermediate Unit" or "CSIU") Social Media Policy is to establish rules and guidance for the use of social media by students, employees, and guests (collectively "Users").

(1.2) A social media blunder is a critical problem with the potential to injure students, employees, guests, and others, to lose confidential information and data, to set back any progress that the Intermediate Unit has previously made, and to subject the User or the Intermediate Unit to litigation.

(2) Definitions

(2.1) ***Guests*** – include, but are not limited to, visitors, workshop attendees, volunteers, adult education staff and students, school board members, independent contractors, vendors, and Intermediate Unit consultants.

(2.2.) ***Social Media***[1] – includes websites that incorporate one or more of the following:

Blogs – are web logs or journals where authors and users can post textual, audio, or video content, and where some permit others to post comments on their blogs. Some websites enable individuals to create free standing blogs, other special interest websites use blog tools and message forums to engage users.

Microblogs – are websites and spaces that allow users to post short blog entries. Twitter is an example, as well as other sites that invite users to post short status and location updates such as Facebook and Foursquare.

Social networks – are websites where users can create customized profiles and form connections with other users based on shared characteristics and interests.

[1] Social media can be engaged in by various ways, for example, through text messages, instant messages, and email by using personal accounts such as Gmail, Yahoo, Hotmail on personally acquired services, systems, and networks, or through text messages, instant messages, and email by using Intermediate Unit accounts on Intermediate Unit services, systems, and networks. Personal digital assistants, cell phones, smartphones, computers, and other devices could be used to engage in social media. As well, chat services such as G-Chat, Blackberry Messenger, and iChat can be utilized. Additional social media may be developed in the future that could be covered by this Policy.

Websites such as Facebook and MySpace tend to foster personal social contact among "friends", while websites such as LinkedIn are oriented toward professional networking. Some intermediate units and businesses are also establishing a presence on social networks.

Media sharing – are websites where users post and share videos, audio files and/or photos as well as tag them to enable searchability. Examples include YouTube, Flickr, Picasa, and Google Video.

Wikis – are resources or documents edited collaboratively by a community of users with varying levels of editorial control by the website publisher. Wikipedia is an example.

Virtual worlds – Web or software-based platforms that allow users to create avatars or representations of themselves, and through these avatars to meet, socialize and transact with other users. Second Life and other virtual worlds are used for social purposes and e-commerce, non-profit fundraising, and videoconferenceing.

Social media includes communication, collaborative sharing, and reaching students, employees and guests for educational purposes using Intermediate Unit provided websites, platforms, resources, or documents. Examples include, but are not limited to, Google Apps, NING, Flat Classroom, Teacher Tube, Moodle, and PAIU created websites such as Keystone Commons, ELLG and New Worlds.

(3) Authority

(3.1) 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 its CIS[2] systems and to monitor, record, check, track, log, access or otherwise inspect *the Intermediate Unit's* CIS systems. In addition, pursuant to 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 User's* personal computers, electronic devices, networks, internet, electronic communication systems, and in databases, files, software, and media that contain Intermediate Unit information and data. Also, pursuant to 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 an Intermediate Unit location, event, or connect it to an 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

[2] "CIS" - computers, network, Internet, electronic communications, information systems, databases, files, software, and media. See CSIU Acceptable Use Policy, Administrative Regulations, and Guidelines # 3515.

Intermediate Unit network, or when using the mobile commuting equipment, telecommunications facilities in 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 pursuant to the law, assist in the protection of the Intermediate Unit's resources, and insure compliance with this Policy, its administrative regulations, and other Intermediate Unit policies, regulations, rules, and procedures, social media and internet service providers terms, and local, state, and federal laws.

(3.2) 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.

Among others the Pennsylvania Code of Professional Practice and Conduct for Educators (22 Pa. Code § 235.2, § 235.4, § 235.5, § 235.10, and § 235.11) and the Pennsylvania School Code (24 P.S. § 9-964) apply.

(4) Delegation of Responsibility

(4.1.) The Intermediate Unit intends to strictly facilitate a learning and teaching atmosphere, to foster the educational purpose and mission of the Intermediate Unit, and to protect its computers, devices, systems, network, information and data against 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 regulations, and to immediately report any violations or suspicious activities to the Executive Director, 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 provided in other relevant Intermediate Unit policies and regulations, rules and procedures.

(4.2.) Employees, students and guests must comply with this Policy, its Social Media Administrative Regulation(s) as well as the CSIU's Acceptable Use Policy # 3515, its accompanying Administrative Regulation # 3515, and Guidelines # 3515, and all other relevant CSIU policies, administrative regulations, rules, procedures, social media terms of use and other legal documents, and local, state and federal laws. In addition, Users may be required to also comply with policies, administrative regulations, rules and procedures at the entity and/or program in which they are assigned. If a User believes there is a conflict in the requirements they are to comply with they must bring the matter to the attention of their supervisor, teacher, or program coordinators who will in turn assist the User.

(4.3.) It is the responsibility of all Users to carefully consider what they place online, including but not limited to, their own behavior when communicating with or "friending" any individual by way of example only, Intermediate Unit or school district students, neighbors, minors, young adults, and adults. The Director of

Technology, or designee, is authorized to access Users' postings on public locations and on Intermediate Unit servers, hard drives, systems, and networks under the direction of the Executive Director, and/or designee, law enforcement, court order, subpoena or other legal action or authority. Users may not coerce others into providing passwords, login, or other security access information to them so that they may access social media or locations that they have no authorization to access. Users should note that information that they place in social media and designate as private can be accessed in litigation, can be distributed by their friends, and can be accessed in other various legal ways.

(4.4.) The Executive Director, and/or designee, is hereby granted the authority to create, publish, and implement additional administrative regulations, procedures, and rules to carry out the purpose of this Social Media Policy. The administrative regulations, procedures, and rules accompanying this Policy must include among other items guidance in implementing and using Intermediate Unit educational social media and commercial social media, and the responsibility of Users for their own behavior when communicating with social media.

(5) Regulations

(5.1.) This Policy, its accompanying administrative regulations, procedures and rules apply to all Intermediate Unit environments, whether the social media is used on Intermediate Unit property, or beyond Intermediate Unit property, in applications, systems, networks that the Intermediate Unit owns, or that are personally operated by Intermediate Unit Users.

(5.2.) It is often necessary to access Users' Intermediate Unit accounts in order to perform routine maintenance and for other legal reasons. 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 Policy, accompanying administrative regulation, the law, and to maintain the system. **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, AND THE INTERMEDIATE UNIT'S AUTHORIZED THIRD PARTY SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THE INTERMEDIATE UNIT'S CIS SYSTEMS. The Intermediate Unit reserves the right to access, view, record, check, receive, monitor, track, log, store, and otherwise inspect and utilize any or all CIS systems, and third party systems, and to monitor and allocate fileserver space. Users of the Intermediate Unit's CIS systems, and third party systems, who transmit or receive communications and information shall be deemed to have consented to having the content of any such communications accessed, viewed, recorded, checked, received, monitored, tracked, logged, stored, and otherwise inspected or utilized by the Intermediate Unit, and to monitor and allocate fileserver space. Passwords**

and message delete functions do not restrict the Intermediate Unit's ability or right to access such communications or information.

(5.3.) Users are responsible for their own behavior when communicating with social media. They will be held accountable for the content of the communications that they state/post on social media locations. Users are responsible for complying with the Intermediate Unit's employee, student, and guest conduct requirements. Users may not disrupt the learning atmosphere, educational programs, school activities, and the rights of others.

Inappropriate communications may not be included in Users social media, including but not limited to (i) confidential, personally identifiable, and sensitive Intermediate Unit information about students, employees, and guests; (ii) child pornography, sexual exploitation, bullying/cyberbullying, inappropriate commercialization of childhood experiences, (iii) defamatory or discriminatory statements and images, (iv) proprietary information of the Intermediate Unit and/or an Intermediate Unit's vendor, (v) infringed upon intellectual property, such as copyright ownership, and circumvented technology protection measures (viii) terroristic threats, and (ix) illegal items and activities.

Users may not use their personal computers, devices, services, systems, and networks during the time they are required to be fulfilling their work, learning, school, or volunteer requirements. The Intermediate Unit blocks students and teachers commercial social media sites on their computers, devices, servers, networks, and systems, therefore Users may not use commercial social media during their work, school responsibilities, and volunteer responsibilities unless approval has been granted by the Telecommunications Manager and the commercial social media has been opened for that person and purpose only. See also relevant parts of Intermediate Unit Policy, Administrative Regulation, and Guidelines 3515.

Where Users place their communication in "privacy" marked social media, they cannot expect that their information will not be disclosed by a person within their "private marked group". Such information may be disclosed by others within the "private group", or the information may be discovered as part of the discovery process in litigation, or it may be disclosed by other means. The Intermediate Unit may be provided this information and be required to investigate it further. Information that the Intermediate Unit obtains may be disclosed without limitation for purposes of investigation, litigation, internal dispute resolution, and legitimate business purposes regardless of whether the particular User is involved.

Information that a User deleted may be recovered indefinitely by the Intermediate Unit.

(5.4.) The Executive Director, or designee, must provide training for employees and instructional sessions for students and, if appropriate, for guests to assist them in knowing the importance of and how to appropriately use social media, and how to

comply with the requirements of this Policy, and its accompanying administrative regulation(s), procedures, and rules.

(5.5.) A User who has a material connection with the Intermediate Unit and endorses an Intermediate Unit product or service may have an obligation to disclose that relationship when the User makes such a statement using social media. The User should contact the Executive Director, and/or designee, to assess the various factors applicable in determining whether disclosure is applicable.

(5.6.) Users may not use the name of the "Central Susquehanna Intermediate Unit" or its logo or mark in any form in social media, on Intermediate Unit internet pages or websites, on websites not owned or related to the Intermediate Unit, or in forums/discussion boards, to express or imply the official position of the 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.

(5.7.) Consequences for Inappropriate, Unauthorized and Illegal Use

General rules for behavior, ethics, and communications apply when using social networking systems and information, in addition to the stipulations of this Policy, its accompanying administrative regulations. Users must be aware that violations of this Policy, accompanying administrative regulation(s), or other Intermediate Unit policies, regulations, rules or procedures, or statutes, regulations and laws or unlawful use of social media systems and information, may result in loss of 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 for employees), dismissal, expulsions, breach of contract, penalties provided in statutes, regulations, and other laws and/or legal proceedings on a case-by-case basis. This Policy, and its accompanying administrative regulation, incorporate 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 Policy, its accompanying administrative regulation, and guidelines, and copyright, property, curriculum, terroristic threat, vendor access, harassment, and discrimination policies.

Further Reference: CSIU Board Policies: 3515, 3521, 3543, 4100, 4112.2, 4112.3, 4115, 4116.11, 4116.13, 4116.23, 4120, 5125.1, 5141.5, 5144.15, 5145, 6000.1

Administrative Regulations/Guidelines: 3515, 3521, 3543, 4100, 4112.2, 4115, 4116.11, 4116.13, 4116.23, 4120, 5145,

Legal Authorization: Public School Code of 1949 – Sections 9-964

Adopted: April 20, 2011

Published: April 21, 2011