CAPITAL AREA INTERMEDIATE UNIT
55 Miller Street, Enola, PA 17025-1640
Phone: (717) 732-8400 www.caiu.org

Acceptable Use of the Communications and Information Systems Policy # 815, Social Media Policy # 815.2 and Social Media Administrative Regulation # 815.2-AR-2

Acknowledgment and Consent Form – 2018-2019

Students

I have received, read, and understand the Acceptable Use of Communications and Information Systems Policy # 815, Social Media Policy # 815.2, and Social Media Administrative Regulation # 815.2-AR-2 and will comply with them. Someone from the Intermediate Unit has also reviewed them with me and my parent(s)/guardian(s) have reviewed them with me. In addition, I have been given the opportunity to obtain information from the Intermediate Unit and my parent(s)/guardian(s) about anything I do not understand, and I have received the information I requested. If I have further questions, I will ask the Director of Technology Services and my parents/guardians. Additionally, I understand that if I violate the Policies, Administrative Regulation, other Intermediate Unit policies, regulations, rules, or procedures I am subject to the Intermediate Unit's discipline up to and including expulsion and could be subject to ISP and website rules, as well as local, state and federal rules and procedures.

_____
Name of Student

_____
Signature of Student

_____
Date of Signature

Parent(s)/Guardian(s)

As the parent/guardian of a student of the Intermediate Unit, I have received, read, and understand the Acceptable Use of the Communications and Information System (CIS) Policy # 815, Social Media Policy # 815.2, and Social Media Administrative Regulation # 815.2-AR-2. In addition, I reviewed the Policies and Administrative Regulation with my child and answered questions s/he asked. If either the child or I have further questions, I will ask the Director of Technology Services. I agree to have my child comply with the requirements of the Policies, Administrative Regulation, other Intermediate Unit policies, regulations, rules, and procedures. Additionally, I understand that if s/he violates the Policies, Administrative Regulation, other Intermediate Unit policies, regulations, rules, or procedures s/he is subject to the Intermediate Unit's discipline, ISP and website rules, as well as local state and federal laws and procedures.

_____
Name of Parent

_____
Signature of Parent

_____
Date of Signature

Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of the Communications and Information Systems
Number	815
Status	Active
Adopted	August 19, 2004
Last Revised	May 26, 2016

TABLE OF CONTENTS

Purpose

The Capital Area Intermediate Unit (Intermediate Unit) provides employees, students, and Guests (Users) with hardware, software, and access to the Intermediate Unit's Electronic Communication System[1] 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, students being served by the Intermediate Unit, workshop attendees, volunteers, adult education staff and students, Board members, independent contractors, and Intermediate Unit consultants and vendors.

Computers, network, Internet, electronic communications, information systems, databases, files, software, and media, collectively called "CIS systems", provide vast, diverse and unique resources. The Intermediate Unit 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, other Intermediate Unit policies, regulations, rules, and procedures, Internet Service Provider (ISP) and website terms, and local, state, and federal laws. For employees, Incidental Personal Use of the Intermediate Unit Computers during breaks, prep time, and lunch is permitted as defined in this Policy. 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 ISP, 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, an event, or connect it to the Intermediate Unit's network.

If Users bring personal Computers or personal electronic devices onto 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, 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 Policy, other Intermediate Unit policies, regulations, rules, procedures, ISP and website terms, and local, state, and federal laws.

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 to immediately report any violations or suspicious activities to the Director of Technology Services, 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, regulations, rules, and procedures.

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][2][3]

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.

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.[4][5]

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; RFID, and 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; Pulse Pens; and any other such technology developed. [1][2][6]

Electronic Communications Systems - any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes. Further, an Electronic Communications System means any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission/transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, 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, text and instant messaging, 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, policies and mission statement.

Harmful to Minors - under federal law, any picture, image, graphic image file or other Visual Depictions that:[2][3]

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.

Under Pennsylvania law, that quality of any depiction or representation in whatever form, of nudity, Sexual Conduct, sexual excitement, or sadomasochistic abuse, when it:[5][7]

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.

Inappropriate Matter - includes, but is not limited to visual, graphic, video, text and any other form of indecent, sexually explicit, Obscene, pornographic, Child Pornographic, or other material that is Harmful to Minors. Examples include: taking, disseminating, transferring, or sharing, whether by electronic transfer (such as sexting, emailing, texting, among others) or otherwise, hateful, illegal, defamatory, lewd, vulgar, profane, inflammatory, threatening, harassing, discriminating (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, bullying/cyberbullying, flagging, terroristic, and other Inappropriate Matter and material specified throughout this Policy, and other Intermediate Unit policies, regulations, rules, and procedures. It also includes advocating the destruction of property.[3][7][8][9][10][11][12][13][14][15][16]

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, or is excessive.

Personal use must comply with this Policy and all other applicable Intermediate Unit policies, regulations, rules, procedures, and ISP and website 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 (CIPA), an individual who has not yet attained the age of seventeen (17). For other purposes, Minor shall mean the age of minority as defined in the relevant law.[1][2][3][7]

Obscene - under federal law, analysis of the material meets the following elements:[2][3][17]

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.

Under Pennsylvania law, any material or performance if:[5][7]

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.

Sexual Act and Sexual Contact - as defined at 18 U.S.C. § 2246(2), and at 18 U.S.C. § 2246(3). [2][3][7][18]

Technology Protection Measure(s) - a specific technology that blocks or filters Internet access to Visual Depictions that are Obscene, Child Pornographic or Harmful to Minors.[3][19]

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, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format, but does not include mere words.[1][17]

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 and website terms, and local, state and federal officials in any investigation concerning or related to the misuse of the CIS systems, or other legal requests, whether criminal or civil actions.[3][20][21][22] [23][24][25][26]

It is often necessary to access Users' 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 Users' accounts for any reason in order to uphold this Policy, regulations, rules, procedures, 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 Policy. 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/guardian) to access bona fide research, not within the prohibitions of this Policy, or for another lawful purpose. No person may have access to material that is illegal under federal or state law.[2][3][25][27]

Expedited review and resolution of a claim that this Policy 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/guardian for a student, and upon the written request from an adult presented to the Director of Student Services or his/her designee.[2][27]

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 programs, 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 ISP, 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, ensure compliance with this Policy, or other Intermediate Unit policies, regulations, rules, and procedures, social media and ISP and website terms, or local, state, and federal laws.

The Intermediate Unit will cooperate to the extent legally required with social media sites, ISPs, 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 supports 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 Policy, other Intermediate Unit policies, regulations, rules, procedures, ISP and website 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 Electronic Communications Systems, including email, text message, and other electronic communications.

4. Remove excess email 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 school district authorities when violation of this and any other applicable Intermediate Unit policies, regulations, rules, and procedures occur or ISP and website terms, 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.

Responsibility

Due to the nature of the Internet as a global network connecting thousands of Computers around the world, Inappropriate Matter, as defined in this Policy, can be accessed through the network and Electronic Communication 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 Policy, and as provided in relevant Intermediate Unit policies, regulations, rules, and procedures.

The Intermediate Unit must publish a current version of this Policy so that all Users are informed of their responsibilities. A copy of this Policy, and the 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.

Delegation of Responsibility

The Director of Technology Services, 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, other Intermediate Unit policies, regulations, rules, and procedures, establish a system to ensure adequate supervision of the CIS systems, maintain executed User Acknowledgement and Consent Forms, and interpret and enforce this Policy, other Intermediate Unit policies, regulations, rules, and procedures.

The Director of Technology Services, 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 Policy and a Records Retention Schedule to include electronically stored information (See Intermediate Unit Policy and Administrative Regulation, 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 policies, regulations, rules and procedures established by the Intermediate Unit, and ISP and website, and, state and federal laws.

The Director of Technology Services, 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.[3][28]

If necessary, the Executive Director is granted the authority to create and enforce an administrative regulation(s) to accompany this Policy.

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.

This Policy, as well as other relevant Intermediate Unit policies, 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. Email and Text Messaging - Intermediate Unit employees may be assigned individual email and text messaging accounts for work-related use and Incidental Personal Use, as needed. Students may be assigned individual email accounts, as necessary, by the Director of Technology Services, and/or designee, and at the recommendation of the teacher who will also supervise the students' use of the email 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 Director of Technology Services, 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 Policy, and all other Intermediate Unit policies (including the Vendor Access Policy), regulations, rules, and procedures, as well as ISP and website terms, state and federal laws, and may not damage the Intermediate Unit's CIS systems. An Intermediate Unit Acknowledgement and Consent Form must be signed in writing or electronically by a Guest, and if the Guest is a Minor, a parent's/guardian's written signature also is required.

4. Blogs - Employees may be permitted to have Intermediate Unit-sponsored blogs, after they receive training, and the approval of the Executive Director, and/or designee. All bloggers must follow the rules provided in this Policy, and all other applicable policies (for example, the Intermediate Unit's Social Media Policy), regulations (for example, the Intermediate Unit's

Social Media Administrative Regulations), rules, and procedures of the Intermediate Unit, ISP and website 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 Executive Director, and/or designee, followed by training authorized by the Intermediate Unit. Users must comply with this 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 and website 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 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/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 Intermediate Unit'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 will 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 will 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 possession and Silent Use[2] of Electronic Communication Devices, including Personal Electronic Communication Devices, by Intermediate Unit students when in compliance with the Electronic Communication Devices Policy, other Intermediate Unit policies, regulations, rules, and procedures, ISP and website terms, and local, state, and federal laws, and supportive of the educational

program of the Intermediate Unit, is permitted. However, the possession and use of Electronic Communication Devices, including Personal Electronic Communication Devices, by students that are found to be disruptive to the educational process and/or environment can be abusive in ways that negatively affect students, employees, and the Intermediate Unit's mission and environment, and therefore, they are prohibited in accordance with this Policy, the Electronic Communication Devices Policy, other Intermediate Unit policies, regulations, rules and procedures, ISP and website terms, and local, state, and federal laws. The Intermediate Unit reserves the right to determine whether the device is disruptive.[6][29]

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 or another entity's equipment.

General Prohibitions –

Users are prohibited from using Intermediate Unit CIS systems to:

1. Communicate about non-work or nonschool-related matters unless the employees' use comports with the definition of Incidental Personal Use in this Policy.

2. Send, receive, view, download, store, access, print, post, 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, emailing, texting, among others). Nor may Users advocate the destruction of property.[6]

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

4. Cyberbully another individual or entity. Intermediate Unit's Bullying/Cyberbullying Policy #249.[13][28]

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 Policy.

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

8. Participate in unauthorized Internet Relay Chats, instant messaging communications and Internet voice communications (online; real-time conversations) that are not for school-related purposes or required for employees to perform their job duties. Students may not use IRCs unless approval has been granted by their teacher/facilitator.

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

10. Communicate through email or text messages for noneducational purposes or activities, unless it is for Incidental Personal Use as defined in this Policy. The use of email to mass mail noneducational or non-work related information is expressly prohibited (for example, the use of the everyone distribution list, all staff lists, building level distribution lists, or other email 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 fundraising or advertising on behalf of the Intermediate Unit and non-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.

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 Copyright Infringement section in this Policy, the Intermediate Unit's Copyright Policy 814, and the Intermediate Unit's Copyright Guidelines Handbook for additional information.[30]

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 Director of Technology Services 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 on the Intermediate Unit's website without administrative approval.

21. Post anonymous messages.

22. Use the name of the "Capital Area 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 Capital Area Intermediate Unit without the expressed, written permission of the Director of Technology Services, 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, SSH terminals, or any website that masks 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 they were yours.[30]

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

Access and Security Prohibitions –

Users must immediately notify the Director of Technology Services, and/or designee, if they have identified a possible security problem. Users must read, understand, and submit a signed Acknowledgement and Consent Form(s), and comply with this Policy 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, which may threaten the health, safety or welfare of any person or persons. Such acts would include, but are not limited to, arranging for a drug sale or the purchase of alcohol, engaging in criminal activity, or being involved in a terroristic threat against any person or property.

6. Disabling or circumventing any Intermediate Unit security, program or device, for example, but not limited to, anti-spyware, anti-spam software, and virus protection software or procedures.

7. Transmitting electronic communications anonymously or under an alias unless authorized by the Intermediate Unit.

8. 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 key logging devices, key logging mechanisms, or key logging 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 immediately reported to the Director of Technology Services, or designee. See the Intermediate Unit's Data Breach Notification Policy 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, 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 Data Breach Notification Policy.

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 retransmission 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 using 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, or 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 Users 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 the consent of the User, and if relevant parent/guardian.

2. Documents, web pages, electronic communications, or videoconferences may not include personally identifiable information that indicates the physical location of a student at a given time without parental/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, 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 sending school districts, outside agencies and the police, the Intermediate Unit's ISP and website terms, and 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 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 Policy and any other Intermediate Unit policy, regulation, rule, or procedure, ISP and website term, or the law may be discovered by routine maintenance and monitoring of the Intermediate Unit CIS system, or any method stated in this Policy, 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. These rights and duties include 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 the 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 ensure compliance with this Policy, other Intermediate Unit policies, regulations, rules, and procedures, ISP and website 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 copyrights will govern the use of material accessed through the Intermediate Unit resources. Users must make a standard practice of requesting permission from the holder of the work, 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.[30][31]

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 unlicensed software – shrink-wrap, clickwrap, browsewrap, and electronic software downloaded from the Internet.[32]

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.

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.[32]

Selection of Material

Intermediate Unit policies, 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 that 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 to present information about the Intermediate Unit under the direction of the Director of Human Resources, and/or designee. Publishers must comply with this Policy, other Intermediate Unit policies, regulations, rules, and procedures, ISP and website 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.

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, may not unlawfully infringe copyrighted material in their blog, and may not disrupt the business or mission of the Intermediate Unit. See also the Intermediate Unit's Social Media Policy, and its accompanying Social Media Administrative Regulations.[33][34]

Contrary conduct will result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section of this Policy, 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 must immediately send or otherwise provide them to the Director of Technology Services, 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 anyway, may not use spyware, cookies, or other program code, key loggers, 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, unless legitimately authorized to do so. Examples of prohibited conduct 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.[3]

If the Intermediate Unit requires that data and information be encrypted, Users must use Intermediate Unit authorized encryption to protect 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(s)/guardian(s) consent.

Cloud, Virtual, and Online Storage of Intermediate Unit Information and Data

Users must keep all Intermediate Unit information (including but not limited to employee and student) information in the Intermediate Unit's and its contracted parties' storage, unless permission is granted in by the Director of Technology Services, and/or designee, or by Intermediate Unit policy. This requirement means that employees, students, and Guests must not place Intermediate Unit information in cloud, virtual, or online storage beyond the control, access, protection, and safety of the Intermediate Unit unless specific permission is granted in writing by the Director of Technology Services, and/or designee, and the student, employee, and Guest agree to the Intermediate Unit's terms and conditions, including but not limited to safety, security, privacy, location, and Intermediate Unit access.

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, other Intermediate Unit policies, regulations, rules, and procedures, ISP and website terms, and local, state, and federal laws. Users must be aware that violations of this 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 Policy incorporates 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 devices, and harassment policies. [20][21][22][23][24]

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 will also be responsible for incidental or unintended damage resulting from negligent, willful or deliberate violations of this Policy, other Intermediate Unit related policies, regulations, rules, and procedures, ISP and website 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 information and/or data contained on them.[19]

Violations as described in this Policy, other Intermediate Unit policies, regulations, rules, and procedures may be reported to a school district, vocational school, and to appropriate legal authorities, whether the ISP or website, 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 cancelation of access to the Intermediate Unit's CIS systems and resources and will subject the User 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, other Intermediate Unit policies, regulations, rules, and procedures, or ISP or website terms, and/or, state, or federal law, must be paid by the User who caused the loss.

---

[1] See *Definition* section for the defined terms generally provided in initial capital letters throughout this Policy.

[2] See Definition section in the Electronic Communication Devices Policy for the defined terms relevant to Electronic Communication Devices and Personal Electronic Communication Devices provided in initial capital letters in this Policy

Legal

1. 18 U.S.C. 2256
2. 20 U.S.C. 6777
3. 47 U.S.C. 254
4. 18 Pa. C.S.A. 6312
5. 24 P.S. 4603
6. Pol. 237
7. 18 Pa. C.S.A. 5903
8. Pol. 103
9. Pol. 103.1
10. Pol. 104
11. Pol. 218.2
12. Pol. 248
13. Pol. 249
14. Pol. 348
15. Pol. 448
16. Pol. 548
17. 18 U.S.C. 1460
18. 18 U.S.C. 2246
19. 24 P.S. 4606
20. Pol. 218
21. Pol. 233
22. Pol. 317
23. Pol. 417
24. Pol. 517
25. 24 P.S. 4604
26. 24 P.S. 510
27. 24 P.S. 4610
28. 24 P.S. 1303.1-A
29. 24 P.S. 1317.1
30. Pol. 814
31. 17 U.S.C. 101 et seq
32. 17 U.S.C. 1202
33. 17 U.S.C. 512
34. Pol. 210.2

24 P.S. 4601 et seq

47 CFR 54.520

Pol. 220

815_TableofContents.pdf (11 KB) 815ATT1.doc (28 KB) 815ATT2.doc (29 KB) 815ATT3.doc (29 KB)

Book	Policy Manual
Section	800 Operations
Title	Social Media Policy
Number	815.2
Status	Active
Adopted	June 28, 2012

Purpose

Both Intermediate Unit educational social media and commercial social media exist for Users to utilize. Therefore, social media could be used either as part of the Intermediate Unit's educational social media to fulfill its mission or for business purposes, or as part of the Users online presence through commercial social media. 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 Capital Area Intermediate Unit ("Intermediate Unit" or "CAIU") Social Media Policy is to establish rules and guidance for the use of social media by students, employees, and guests (collectively "Users").

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.

Definitions

Guests - include, but are not limited to, visitors, workshop attendees, volunteers, adult education staff and students, Board members, independent contractors, vendors, and Intermediate Unit consultants.

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. 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 videoconferencing.

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, Twitter, Wikispaces, iTunes University, Pinterest, Four Square, and YouTube.

Authority

The Intermediate Unit has the right, but not the duty, to inspect, review, or retain electronic communication created, sent, displayed, received, and/or stored on and over the Intermediate Unit’s CIS^2 systems and devices and to monitor, record, check, track, log, access or otherwise inspect its CIS systems and devices.

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 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 and 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, ensure compliance with this Policy, its administrative regulations, 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.

Delegation of Responsibility

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 as well as the CAIU's Acceptable Use Policy # 815, and all other relevant CAIU policies, administrative regulations, rules, procedures, social media terms of use and other legal documents, and local, state and federal laws.

Users must immediately report any violations or suspicious activities to their immediate supervisor, 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. 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 administrator who will in turn assist the User.

It is the responsibility of all Users to carefully consider their behavior and what they place online when communicating with or "friending" any individual. The Director of Human Resources, and/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, a court order, a 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.

The Executive Director, and/or designee, is hereby granted the authority to create 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.

Guidelines

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 regulations, 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 PARTIES' SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THESE 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 authorized third parties' 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.

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, and fulfilling their Immediate Unit employee, student, and guest responsibilities. 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, or guest responsibilities, unless approved by the Intermediate Unit, and/or its designee. The Intermediate Unit, at its discretion, retains the right to block all commercial social media sites on its computers, devices, servers, networks, and systems; however the Intermediate Unit may choose to unblock such sites at its discretion, or at the request of a User, if the use is related to the User fulfilling their employee, learning, or guest responsibility. Users may not use commercial social media during their work, school, and guest responsibilities unless approval has been granted by their supervisor/teacher, and/or designee, and the commercial social media has been opened for that person(s) and purpose only (see also relevant sections of the Acceptable Use Policy # 815).

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 CAIU.

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.[1]

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.

Users may not use the name of the "Capital Area 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.

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 and 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, federal, state, and local 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, up to and including termination in accordance with the CAIU Progressive Disciplinary Process; 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(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, acceptable use, copyright, property, curriculum, terroristic threat, vendor access, harassment, and discrimination policies.[2][3] [4][5][6]

Further Reference: CAIU Board Policies, Administrative Regulations, Rules, and Procedures

[1] It is possible that social media could be engaged in by various ways, for example, through text messages, instant messages, and email by using personal accounts such as Gmail, Yahoo, and Hotmail on personally acquired services, systems, and networks, and/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 iMessage, G-Chat, Blackberry messenger, iChat, and FaceTime could be utilized. Additional social media may be developed in the future that could be covered by this Policy.

[2] "CIS" - computers, network, Internet, electronic communications, information systems, databases, files, software, and media. See CAIU Acceptable Use Policy # 815.

Legal

1. 47 U.S.C. 254
2. 22 PA Code 235.10
3. 22 PA Code 235.11
4. 22 PA Code 235.2
5. 22 PA Code 235.4
6. 22 PA Code 235.5