

<p>3. Authority</p> <p>24 P.S. § 5-510</p> <p>22 Pa. Code §§ 235.2, 235.4,</p>	<p>blogs. Some websites enable individuals to create free standing blogs, other special interest websites use blog tools and message forums to engage users.</p> <p><u>Microblogs</u> – 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.</p> <p><u>Social networks</u> – 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 schools and businesses are also establishing a presence on social networks.</p> <p><u>Media sharing</u> – 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.</p> <p><u>Wikis</u> – 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.</p> <p><u>Virtual worlds</u> – 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.</p> <p>Social media includes communication, collaborative sharing, and reaching students, employees and guests for educational purposes using School provided websites, platforms, resources, or documents. Examples include but are not limited to: Google Apps, Ning, TeacherTube, Moodle, Schoolwires.</p> <p>The School has the right, but not the duty, to inspect, review, or retain electronic communication created, sent, displayed, received or stored on and over the School’s CIS² systems and to monitor, record, check, track, log, access or otherwise inspect its CIS systems.</p> <p>In addition, pursuant to the law, the School has the right, but not the duty, to inspect, review, or retain electronic communication created, sent, displayed,</p>
--	--

² “CIS” - computers, network, Internet, electronic communications, information systems, databases, files, software, and media. See Monroe Career and Technical Institute’s Policy #815.

<p>235.5, 235.10, 235.11</p> <p>4. Delegation of Responsibility</p>	<p>received or stored on User’s personal computers, electronic devices, networks, Internet, electronic communication systems, and in databases, files, software, and media that contain School information and data.</p> <p>Also, pursuant to the law, the School 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 School location, event, or connect it to the School network and/or systems, and/or that contains School programs, or School data or information.</p> <p>The above applies no matter where the use occurs whether brought onto School property, to School events, or connected to the School network, or when using mobile commuting equipment and 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 School’s resources, insure compliance with this Policy, its Administrative Regulations or other School policies, regulations, rules, and procedures, social media and internet service providers terms, or local, state, and federal laws.</p> <p>The School will cooperate with social media sites, internet service providers, local, state, and federal officials to be reasonably cooperative in investigations or with other legal requests, whether criminal or civil actions.</p> <p>The School intends to strictly facilitate a learning and teaching atmosphere, to foster the educational purpose and mission of the School, 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 School 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 MCTI’s Policy # 815, and all other relevant MCTI policies, Administrative Regulations, rules, procedures, social media terms of use and other legal documents, and local, state and federal laws.</p> <p>Users must immediately report any violations or suspicious activities to the 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 School policies and regulations, rules and procedures. <u>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</u></p>
---	--

<p>5. Regulations</p>	<p><u>their supervisor, teacher, or administrator who will in turn assist the User.</u></p> <p>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 Technology, or designee, is authorized to access Users’ postings on public locations and on School servers, hard drives, systems, and networks under the direction of the 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.</p> <p>The 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 School District educational social media and commercial social media, and the responsibility of Users for their own behavior when communicating with social media.</p> <p>It is often necessary to access Users’ School 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 SCHOOL’S CIS SYSTEMS, AND THE SCHOOL’S AUTHORIZED THIRD PARTIES’ SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THESE SYSTEMS. The School 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 School’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 School, and to the School monitoring and allocating fileserver space. Passwords and message delete functions do not restrict the School’s</p>
-----------------------	---

<p>47 U.S.C. § 254 (5)(B)(iii)</p>	<p>ability or right to access such communications or information.</p> <p><u>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.</u> Users are responsible for complying with the School’s employee, student, and guest conduct requirements. Users may not disrupt the learning atmosphere, educational programs, school activities, and the rights of others.</p> <p>Inappropriate communications may not be included in Users social media, including but not limited to (i) confidential, personally identifiable, and sensitive School 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 School and/or a School’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.</p> <p>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 responsibilities, or volunteer requirements. The School blocks all commercial social media sites on its computers, devices, servers, networks, and systems, therefore Users may not use commercial social media during their work, school, and volunteer responsibilities unless approval has been granted by the Director, and/or designee, and the commercial social media has been opened for that person(s) and purpose only (see also relevant sections of Policy 815).</p> <p>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 School may be provided this information and be required to investigate it further. Information that the School 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.</p> <p>Information that a User deleted may be recovered indefinitely by the School.</p> <p>The Director, or designee, must provide training for employees and instructional sessions for students and, if appropriate, for guests to assist them in</p>
--	---

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.

A User who has a material connection with the School and endorses a School 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 Director, and/or designee, to assess the various factors applicable in determining whether disclosure is applicable.

Users may not use the name of the “Monroe Career and Technical Institute” or its logo or mark in any form in social media, on School internet pages or websites, on websites not owned or related to the School, or in forums/discussion boards, to express or imply the official position of the School without the expressed, written permission of the Director, and/or designee. When such permission is granted, the posting must state that the statement does not represent the position of the School.

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 School 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, oral or written reprimands, student suspensions or expulsions, position reassignment, employee suspensions (with or without pay), dismissal, breach of contract, penalties provided in statutes, regulations, and other laws and/or legal proceedings. This will be handled on a case-by-case basis. This Policy, and its accompanying Administrative Regulation, incorporate all other relevant School policies, such as, but not limited to, (we don’t have these) the student and professional employee discipline policies, Code of Student Conduct, Acceptable Use Policy, its accompanying Administrative Regulations and guidelines, and copyright, property, curriculum, terroristic threat, vendor access, harassment, and discrimination policies.

Further Reference: MCTI Policies: 103 and accompanying policies, 113.1, 207, 216.1, 218 and accompanying policies, 219, 220, 233, 235, 237, 248 and accompanying administrative regulation, 249, 815 and accompanying documents, 907.