WESTMORELAND INTERMEDIATE UNIT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF COMMUNICATIONS AND INFORMATION SYSTEMS

ADOPTED: JUNE 25, 2013

REVISED:

815. ACCEPTABLE USE OF COMMUNICATIONS AND INFORMATION SYSTEMS

1. Purpose

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

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

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

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

	to the Intermediate Unit network. If Users' bring personal Computers or personal electronic devices onto the Intermediate Unit property, to Intermediate Unit events, or connect them to the Intermediate Unit's network and systems, and if the Intermediate Unit reasonably believes the personal Computers and/or personal electronic devices contain Intermediate Unit information or contain information that violates a Intermediate Unit policy or administrative regulation, the legal rights of the Intermediate Unit or another person, or involves significant harm to the Intermediate Unit or another person, or involves a criminal activity, the personal Computers or personal electronic devices may be legally accessed *in accordance with the law* to insure compliance with this policy, accompanying administrative regulation, and other Intermediate Unit policies, regulations, rules, procedures, ISP terms, and local, state, and federal laws. Users may not use their personal Computers and personal technology electronic devices to access the Intermediate Unit's intranet, Internet or any other CIS system unless approved by the Supervisor of Information Technology, and/or designee. The Intermediate Unit intends to strictly protect its CIS systems against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting these Intermediate Unit assets and in lessening the risks that can destroy these important and critical assets. Consequently, Users are required to fully comply with this Policy and its accompanying administrative regulation(s), and to immediately report any violations or suspicious activities to the Supervisor of Information Technology, 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, and procedures.
2. Authority 47 U.S.C. § 254(1) 24 P.S. § 510 24 P.S. § 4604	Access to the Intermediate Unit's CIS systems through school resources is a privilege, not a right. These, as well as the User accounts and information, are the property of the Intermediate Unit, which reserves the right to deny access to prevent unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The Intermediate Unit will cooperate to the extent legally required with other educational entities, ISP, local, state and federal officials in any investigation concerning or related to the misuse of the CIS systems. 47 U.S.C. § 254(l); 24 P.S. § 510; 24 P.S. § 4604. It is often necessary to access User accounts in order to perform routine maintenance and security tasks. System administrators have the right to access by interception, and to access the stored communication of User accounts for any reason in order to uphold this Policy, administrative regulation, 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.
20 U.S.C. § 6777 47 U.S.C. § 254 24 P.S. § 4604	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 and its accompanying administrative regulation. Measures designed to restrict adults' and Minors' access to material Harmful to Minors may be disabled to enable an adult or a student (who has provided written consent from a parent or guardian) to access *bona fide* research, not within the prohibitions of this Policy, its accompanying administrative regulation(s) and guidelines, or for another lawful purpose. No person may have access to material that is illegal under federal or state law. 20 U.S.C. § 6777; 47 U.S.C. § 254; 24 P.S. § 4604.
20 U.S.C. § 6777(c) 24 P.S. § 4610	Expedited review and resolution of a claim that this Policy and/or its administrative regulation is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee, upon the receipt of written consent from a parent or guardian for a student, and upon the written request from an adult presented to the Supervisor of Information Technology. 20 U.S.C. § 6777(c); 24 P.S. § 4610. The Intermediate Unit has the right, but not the duty, to inspect, review, or retain Electronic Communication created, sent, displayed, received or stored on and over *the Intermediate Unit's* CIS systems and to monitor, record, check, track, log, access or otherwise inspect its CIS systems. In addition, *in accordance with the law*, the Intermediate Unit has the right, but not the duty, to inspect, review, or retain Electronic Communications created sent, displayed, received, or stored *on User's* personal computers, electronic devices, networks, Internet, Electronic Communications Systems, and in databases, files, software, and media that contain Intermediate Unit information and/or data.

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

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

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, its accompanying administrative regulation, other Intermediate Unit policies, regulations, rules, procedures, ISP terms, and local, state, or federal law.

The Intermediate Unit additionally reserves the right to:

1. Determine which CIS systems' services will be provided through Intermediate Unit resources.
2. Determine the types of files that may be stored on Intermediate Unit file servers and Computers.

	3. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network and communications systems, including e-mail, text messages, and other Electronic Communications. 4. Remove excess e-mail and other Electronic Communications or files taking up an inordinate amount of fileserver disk space after a reasonable time. 5. Revoke User privileges, remove User accounts, or refer to legal authorities, and/or Intermediate Unit authorities when violation of this and any other applicable Intermediate Unit policies, administrative regulations, rules, and procedures occur or ISP terms, local, state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, social media, vendor access, data breach, and destruction of Intermediate Unit resources and equipment.
3. Delegation of Responsibility	The Supervisor of Information Technology, and/or designee, will serve as the coordinator to oversee the Intermediate Unit's CIS systems and will work with other regional or state organizations as necessary to educate Users, approve activities, provide leadership for proper training for all Users in the use of the CIS systems and the requirements of this Policy, and its accompanying administrative regulation, establish a system to insure adequate supervision of the CIS systems, maintain executed *User Acknowledgement and Consent Forms*, and interpret and enforce this Policy, and its accompanying regulation(s). The Supervisor of Information Technology, and/or designee, will establish a process for setting-up individual and class accounts, set quotas for disk usage on the system, establish Record Retention and Records Destruction Policies and a Records Retention Schedule to include electronically stored information, and establish the Intermediate Unit virus protection process. Unless otherwise denied for cause, student access to the CIS systems resources must be through supervision by the professional staff. Administrators, teachers and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of the resources. All Users have the responsibility to respect the rights of all other Users within the Intermediate Unit and the Intermediate Unit CIS systems, and to abide by the rules established by the Intermediate Unit, the school district(s), its ISP, local, state and federal laws.
47 U.S.C. § 254 (5)(B)(iii) 24 P.S. § 1303.1-A	The Executive Director, and/or designee, has the responsibility to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. 47 U.S.C. § 254 (5)(B)(iii); 24 P.S. § 1303.1-A.

	The Executive Director is granted the authority to create an administrative regulation to accompany this Policy. The administrative regulation must include, but is not limited to, the following sections: Purpose, Definitions, Responsibility, and Guidelines including but not limited to, Prohibitions (*General Prohibitions, Access and Security Prohibitions, and Operational Prohibitions*), Content Guidelines, Due Process, Search and Seizure, and Selection of Material. Additional sections may be included in the administrative regulation at the discretion of the Executive Director. This Policy must be incorporated into its accompanying administrative regulation.
4. Guidelines	Access to the CIS Systems The CIS systems accounts of Users must be used only by authorized owners of the accounts and only for authorized purposes. An account will be made available according to a procedure developed by appropriate Intermediate Unit authorities. The Intermediate Unit's Acceptable Use of Communications and Information Systems Policy, its accompanying administrative regulation, as well as other relevant Intermediate Unit policies, administrative regulations, rules, and procedures, will govern use of the Intermediate Unit's CIS systems for Users. Types of Services include, but are not limited to: 1. Internet - Intermediate Unit employees, students, and Guests will have access to the Internet through the Intermediate Unit's CIS systems, as needed. 2. E-Mail and Text Messaging - Intermediate Unit employees may be assigned individual e-mail and text messaging accounts for work-related use, as needed. Students may be assigned individual e-mail accounts, as necessary, by the Supervisor of Information Technology and/or designee, and at the recommendation of the teacher who will also supervise the students' use of the e-mail service**.** Students and Guests may not be assigned text message accounts. 3. Guest Accounts - Guests may receive an individual Internet account with the approval of the Supervisor of Information Technology 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, its accompanying administrative regulation, and all other Intermediate Unit policies (including the Vendor Access Policy), procedures, and rules, as well as Internet Service Provider ("ISP") terms, local, state and federal laws and may not damage the Intermediate Unit's CIS systems.

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

5. Web 2.0 Second Generation Web-based Services - Certain Intermediate Unit authorized Second Generation Web-based services, such as social networking sites, wikis, podcasts, RSS feeds, social software, folksonomies and collaboration tools that emphasize online educational collaboration and sharing among Users may be permitted by the Intermediate Unit, however, such use must be approved by the Supervisor of Information Technology and/or designee, followed by training authorized by the Intermediate Unit. Users must comply with this Policy, its accompanying administrative regulation, as well as any other relevant policies (including the Intermediate Unit's Social Media Policy), regulations (for example, the Intermediate Unit's Social Media Administrative Regulations) rules, and procedures including the copyright, ISP terms, and local, state, and federal laws during such use.

Parental Notification and Responsibility

The Intermediate Unit will notify the parents/guardians about the Intermediate Unit CIS systems and the policies, regulations, rules, and procedures governing their use. This Policy, and its accompanying administrative regulation, contain restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the Intermediate Unit to monitor and enforce a wide range of social values in student use of the Internet. Further, the Intermediate Unit recognizes that parents and guardians bear primary responsibility for transmitting their particular set of family values to their children. The Intermediate Unit will encourage parents/guardians to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the School's District's CIS system. Parents/Guardians are responsible to help monitor their children's use of the Intermediate Unit's CIS systems when they are accessing the systems.

Intermediate Unit Limitation of Liability

The Intermediate Unit makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the Intermediate Unit's CIS

systems will be error-free or without defect. The Intermediate Unit does not warrant the effectiveness of Internet filtering. The electronic information available to Users does not imply endorsement of the content by the Intermediate Unit, nor is the Intermediate Unit responsible for the accuracy or quality of the information obtained through or stored on the CIS systems. The Intermediate Unit shall not be responsible for any damage Users may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using the Computers, network and Electronic Communications Systems. The Intermediate Unit shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The Intermediate Unit shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the Intermediate Unit's CIS systems. In no event shall the Intermediate Unit be liable to the User for any damages whether direct, indirect, special or consequential, arising out the use of the CIS systems.

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 in the accompanying administrative regulation(s). The Intermediate Unit reserves the right to determine if any activity not appearing in the lists 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 computing 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 school district's equipment. Students must also comply with the Intermediate Unit's Electronic Devices Policy, #237.

Copyright Infringement and Plagiarism

Federal laws, cases, policies, regulations, and guidelines pertaining to copyright will govern the use of material accessed through the Intermediate Unit resources. See Policy # CP-2012. Users will make a standard practice of requesting permission from the holder of the work, or complying with the Fair Use Doctrine, and/or complying with license agreements. Employees will instruct Users to respect copyrights, request permission when appropriate, and to comply with the Fair Use Doctrine, and/or license agreements. Employees will respect and comply as well. 17 U.S.C. § 101 et seq.; Policy # 814.

Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing the law. The Intermediate Unit does not permit illegal acts pertaining to the copyright law. Therefore, any User violating the copyright law does so at their own risk and assumes all liability.

Violations of copyright law include, but are not limited to, making unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over Computer networks, remixing or preparing mash-ups that violate the law, and deep-linking and framing into the content of others' websites. Further, the illegal installation of copyrighted software or files for use on the Intermediate Unit's Computers is expressly prohibited. This includes all forms of licensed software – shrink-wrap, clickwrap, browsewrap, and electronic software downloaded from the Internet.

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

Intermediate Unit guidance on plagiarism will govern use of material accessed through the Intermediate Unit's CIS systems. Users must not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices. Users understand that use of the Intermediate Unit's CIS systems may involve the Intermediate Unit's use of plagiarism analysis software being applied to their works. Policy # 814.

<u>Intermediate Unit Website</u>

The Intermediate Unit has established and maintains a Website and will develop and modify its web pages that will present information about the Intermediate Unit under the direction of the Supervisor of Information Technology, and/or designee. Publishers must comply with this Policy, its accompanying regulation, other Intermediate Unit policies, regulations, rules, procedures, ISP terms, and local, state, and federal laws.

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

<u>Blogging</u>

If an employee, student or Guest creates a blog with their own resources and on their

own time, the employee, student, or Guest may not violate the privacy rights of employees and students, may not use Intermediate Unit personal and private information/data, images, equipment, resources, and copyrighted material in their blog, and may not disrupt the Intermediate Unit. See also the Intermediate Unit's Social Media Policy # 816, and its accompanying administrative regulations.

Contrary conduct will result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section of this 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 Supervisor of Information Technology and/or designee.

The Intermediate Unit will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

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

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

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

Consequences for Inappropriate, Unauthorized and Illegal Use

General rules for behavior, ethics, and communications apply when using the CIS systems and information, in addition to the stipulations of this Policy, its accompanying administrative regulation, other Intermediate Unit policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws. Users must be aware that violations of this Policy 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 device, and harassment policies.

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

Violations as described in this Policy, its accompanying administrative regulation, other Intermediate Unit policies, regulations, rules, and procedures may be reported to the Intermediate Unit, and to appropriate legal authorities, whether the ISP, local, state, or federal law enforcement. Actions that constitute a crime under state and/or federal law, could result in arrest, criminal prosecution, and/or lifetime inclusion on a sexual offenders registry. The Intermediate Unit will cooperate to the extent legally required with authorities in all such investigations.

Vandalism will result in cancellation of access to the Intermediate Unit's CIS systems and resources and is subject to discipline.

Any and all costs incurred by the Intermediate Unit for repairs and/or replacement of software, hardware and data files and for technological consultant services due to any violation of this Policy, its accompanying administrative regulation, other Intermediate Unit policies, regulations, rules, and procedures, or ISP terms, or federal, state, or local law, shall be paid by the User who caused the loss.

References:

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