EASTERN WESTMORELAND CAREER & TECHNOLOGY CENTER

SECTION: OPERATIONS

TITLE: USE OF TECHNOLOGY RESOURCES/ACCEPTABLE USE OF INTERNET

ADOPTED: AUGUST 19, 2015

REVISED:

815. USE OF TECHNOLOGY RESOURCES/ACCEPTABLE USE OF INTERNET

1. Purpose

The Joint Operating Committee of the Eastern Westmoreland Career and Technology Center supports and encourages the use of technology to aid in educational and operational processes of the center. The Joint Operating Committee recognizes the vast and unique resources that Internet access offers to both students and teachers. The Joint Operating Committee has consistently encouraged the use of Internet technology to aid in and promote the overall educational experience. The Joint Operating Committee further recognizes that the Internet allows for access to virtually unlimited information as well as the ability to communicate with individuals and institutions worldwide.

The Joint Operating Committee also recognizes the potential for misuse of the various technology resources supplied to students, faculty and staff. Nevertheless, it is the belief of the Joint Operating Committee that the value of technology in the educational process outweighs the potential risk of misuse. The Joint Operating Committee is, however, committed to a policy which seeks to discourage, minimize and avoid any misuse by students, faculty and staff.

2. Definitions

The term child pornography is defined under both federal and state law.

18 U.S.C. Sec. 2256

Child pornography - under federal law, is 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. 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.
18 Pa. C.S.A. Sec. 6312	Child pornography - under state law, is 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. The term harmful to minors is defined under both federal and state law.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that: 1. Taken as a whole, with respect to minors, appeals to a 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 contact, 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 or scientific value as to minors.
18 Pa. C.S.A. Sec. 5903	Harmful to minors - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it: 1. Predominantly appeals to the prurient, shameful, or morbid interest of minors; 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.
18 Pa. C.S.A. Sec. 5903	Obscene - any material or performance, if: 1. The average person applying contemporary community standards would find that the subject matter 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.
47 U.S.C. Sec. 254	Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.
3. Authority	Use of technology resources by students, faculty and staff shall be considered a privilege, which may be denied or limited where violation of this policy occurs. The center reserves the right to control, monitor, log and restrict in size or content all network use, email and space available on center work stations or servers. The center reserves the right to log network use, Internet activity, and email fileserver space. In addition, the center will periodically delete all email from all email accounts in order to preserve fileserver space. Archives of email messages will be maintained by the center for the duration of one (1) year. Student email will not be archived. Network administrators may review student and staff files and communications to maintain system integrity and ensure that students and staff are using the system only for appropriate uses. It is the policy of the center to protect technology users from harassment, unwanted and improper communication and violations of their privacy. The center receives Internet access to its students, teachers and administrators through the Westmoreland Intermediate Unit. As a participating career and technology center within the Westmoreland Intermediate Unit, the center must include the Westmoreland Intermediate Unit's Acceptable Use Policy as the minimum level of requirements for use of the Internet. The center acknowledges and incorporates the Westmoreland Intermediate Unit's Acceptable Use Policy within this policy. (A copy of the Westmoreland Intermediate Unit Internet Acceptable Use Policy is attached and made a part of this policy). The center shall not be responsible for unauthorized charges or fees resulting from inappropriate use of or access to the Internet or any other technology resource. Information available to students and staff through various technology resources does not imply endorsement of the content of that information by the center, nor does the center guarantee the accuracy of that information. The center shall not be responsible for information which is lost, damaged or unavailable when using technology resources. This policy covers the use of all center-owned electronic communications systems or technology devices: email, Internet access, center Internet, center -wide telephone systems, and all licensed software programs, whether or not they are associated with any of the above-mentioned systems. This policy also covers the use of all noncenter

	owned or personal devices whether access is via the center network resources or through an independent vendor. The center recognizes the importance of teaching acceptable use and online safety to students. The center curriculum shall include instruction for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. <u>Filtering</u>
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 20 U.S.C. Sec. 6777	All Eastern Westmoreland Career and Technology Center computers with Internet access shall be equipped with filtering software. The Children's Internet Protection Act requires that filtering be on all computers with Internet access regardless of whether they are used by students or staff. In an effort to block and filter inappropriate material that may otherwise be accessible via the Internet, the center, through the Westmoreland Intermediate Unit, has internet filtering services in effect that are fully compliant with the Children's Internet Protection Act.
24 P.S. Sec. 4604	Upon request by students or staff, the Administrative Director or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.
24 P.S. Sec. 4610 20 U.S.C. Sec. 6777	In keeping with the above guidelines of the Children's Internet Protection Act, the filtering service may be disabled on computers by the network administrator, an adult administrator, or a teacher for bona fide research or other lawful purposes. The filtering service may not be disabled by students or other minors for any reason.
4. Delegation of Responsibility 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 CFR Sec. 54.520	The Administrative Director or designee shall be responsible for recommending technology and developing procedures used to determine whether the center's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to: 1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Joint Operating Committee.

	2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
47 U.S.C. Sec. 254	The Administrative Director or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including: 1. Interaction with other individuals on social networking websites and in chat rooms.
SC 1303.1-A Pol. 249	2. Cyberbullying awareness and response.
5. Guidelines	<u>Responsibilities Of All Users Of Technology</u> Students, faculty, staff and any other user of the Internet or other technology resources provided by the center shall act in a responsible, ethical and legal manner in accordance with this policy, the accepted rules of network and Internet etiquette as well as state and federal laws. All center-affiliated users must sign the Technology Resource Use Agreement to verify that they will abide by the rules set forth within this policy. Until this signed form is returned by the user and/or parent/guardian to the center Technology Department, network access will be suspended. Parental consent shall be required for students before Internet access is granted. This form will be included as part of the student handbook and should be submitted to the respective school building at the beginning of each school year. (A copy of the Technology Resource Use Agreement is attached and made a part of this policy). Staff members must sign appropriate use agreement(s) as designated by the Administrative Director The guidelines set forth below shall be followed by students, faculty, staff, and any technology user. All users are prohibited from using the Internet, email or any technology resources for: 1. Commercial, private, advertisement or for-profit purposes. 2. Lobbying or political purposes. 3. Any illegal purpose.

	4. The dissemination of hate mail, discriminatory remarks and offensive or inflammatory communications.
	5. The unauthorized or illegal installation, distribution or a reproduction of copyrighted materials. This includes but is not limited to downloading copyrighted music files, creating P2P networks and/or applications over the network, or streaming video or audio that is not educational.
Pol. 237	6. Gaining access to obscene or pornographic material of any kind.
	7. Gaining access to material that is harmful to students and minors or which has been deemed inappropriate for students and minors by other Joint Operating Committee policies of the center.
	8. Transmitting inappropriate language or profanity.
	9. Transmitting material likely to be offensive or objectionable to recipients of the material.
	10. Obtaining or modifying files, passwords and data belonging to other users.
	11. Impersonating another user, anonymity and pseudonyms.
	12. Loading or using unauthorized program files, games or electronic media.
	13. Disrupting the work of other users.
	14. The destruction, modification, abuse or unauthorized access to network hardware, software and other files.
	15. The quoting of personal communications or works in a public forum without the prior consent of the author.
	16. Gaining access to sexually oriented chat rooms, email exchanges or any other information of a sexually oriented, obscene, pornographic or extremely violent nature.
	17. The purpose of tampering, interfering or intercepting another user's email.
	18. Disabling or circumventing or attempting to disable or circumvent Internet filtering.
SC 1301.1-A Pol. 249	19. Bullying/Cyberbullying
	20. Users shall not reveal their passwords to any other individual.

	21. Users shall not use a computer which has been logged on under another person's name. Safety It is the center's goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, email, social networking websites, etc.
47 U.S.C. Sec. 254 47 CFR Sec. 54.520	Internet safety measures shall effectively address the following: 1. Control of access by minors to inappropriate matter on the Internet and World Wide Web. 2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications. 3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities. 4. Unauthorized disclosure, use, and dissemination of personal information regarding minors. 5. Restriction of minors' access to materials harmful to them.
	Content Guidelines Information electronically published on the center's computers, network, Internet, electronic communications and information 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 child's phone number, street address, or box number, name (other than first name) or the names of family members without parental consent. 2. Documents, web pages, electronic communications, or videoconferences may not include identifiable information that indicates the physical location of a student at a given time without parental consent. 3. Documents, web pages, electronic communications, or videoconferences may

	not contain objectionable material or point directly or indirectly to objectionable materials.
Pol. 814	4. Documents, web pages and electronic communications must conform to all center policies and guidelines, including copyright.
	Security And Privacy
	Security on any computer system is high priority, especially when the system involves many users. If any user can identify a security problem on the center network, s/he must notify a network administrator. Do not demonstrate the problem to others.
	As a user of this system, users should notify a network administrator of any violations of this policy taking place by other users or outside parties. This may be done anonymously.
	To the extent required, users of the center's technology systems shall be protected from harassment or commercially unsolicited electronic communication. Any user who receives threatening or unwelcome communications must immediately take them to the Technology Coordinator.
	Users may not steal another's identity in any way, may not use spyware, parasite ware, cookies, or use center or personal employee technology or resources in any way to invade one's privacy. Additionally, the user many not disclose, use or disseminate confidential and personal information about students or employees (examples include, but are not limited to, using a cell phone with camera and Internet access to take pictures of anything, including but not limited to, persons, places, and documents relevant to the center; saving, storing and sending the image with or without text or disclosing them by any means, including but not limited to, print and electronic matter; revealing students grades; social security numbers; 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 center unless authorized to do so).
	Students may be asked by their teachers to participate in Web 2.0 online collaborative environments (wikis, blogs, chats, discussion boards, etc.). These tools shall only be used to cover and discuss educational topics to enhance learning inside and outside of the classroom. In accordance with CIPA guidelines, users under the age of thirteen (13) shall not participate in Web 2.0 environments unless part of Eastern Westmoreland Career and Technology Center's approved online curricular program.

Students shall not agree to meet with someone they have met online unless they have parental consent.

In order for the center to use student images in video form, hard copy publications, and/or the center's web site, parental consent must be given by signing the Photo/Video Release Form. This form will be included as part of the student handbook and should be submitted to the respective school building at the beginning of each school year.

Technology Devices

The policy setting forth the financial responsibility for loss, destruction or damages to technology equipment shall be as follows:

1. In all cases of destruction or damage to any technology device, the center Technology Department shall investigate and determine whether the destruction or damage resulted from intentional or malicious conduct. The building administrator's decision in this regard shall be final.

2. If the damage or destruction resulted from intentional or malicious conduct, the student, and his/her parent/guardian, causing the destruction or damages shall be responsible for the entire amount.
3. Parents/Guardians shall be responsible for the entire value where the technology device is lost or stolen, regardless as to whether malicious or intentional conduct was involved. Parents/Guardians are advised to determine whether their homeowner's or renter's insurance provides coverage for the loss or theft of a school laptop computer.

4. The Technology Department shall complete repairs or have them completed in the most cost-effective manner, and shall charge for labor and replacement parts.

5. The center shall not be responsible for the safety, security, loss, or damage of personal electronic devices that students choose to bring to school. In addition, the center does not provide personal property insurance for any personally owned device. Such insurance can be obtained by an independent carrier.

Faculty Technology Devices

When possible, the center shall provide a technology device to faculty needing to perform expected daily tasks. Faculty shall demonstrate proper care of the technology device to increase the longevity of the machine. Before any technology device and access are given, the employee shall sign the Technology Resources Use Agreement For Faculty.

	The policy setting forth the responsibility for loss, destruction or damages to technology devices assigned by the center to faculty members shall be as follows: 1. In all cases of destruction or damage to a technology device, the Technology Director and the Technology Department shall investigate and determine whether the destruction or damage resulted from intentional or malicious conduct. 2. If the damage or destruction resulted from intentional or malicious conduct, the faculty member who caused the destruction or damage shall be responsible for the cost of repairs, or if necessary replacement of the technology device. 3. The center's Technology Department shall complete repairs and have them completed in the most cost-effective manner. 4. Faculty members shall be responsible for the entire value of the technology device, and are expected to take every precaution to ensure the care of the device. If it is determined that negligence contributed to the loss or theft, the faculty member shall be held responsible for the entire value of the technology device. 5. In the case of a lost or stolen technology device, faculty members are advised to contact their homeowner's or renter's coverage prior to any payments being made to the center. <u>Penalty For Violation Of This Policy</u>
Pol. 218, 233	Violations of this policy shall be disciplined in accordance with the provisions of the existing policy for student discipline. Along with the disciplinary response under that policy, the following may be imposed: 1. The user shall be responsible to make full restitution for any damage (including all labor costs for repair or replacement) to equipment, software and any other part of the network resulting from known improper use or deliberate or willful acts. 2. Any acts which may violate state or federal laws including but now limited to copyrights violations, theft and destruction of property shall be reported to the appropriate authorities for possible persecution. 3. The user may lose access privileges temporarily or on a permanent basis.
Pol. 317	Staff or employees violating this policy may be disciplined in accordance with center policy.

	References: School Code – 24 P.S. Sec. 1303.1-A PA Crimes Code – 18 Pa. C.S.A. Sec. 5903, 6312 Child Internet Protection Act – 24 P.S. Sec. 4601 et seq. U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq. Sexual Exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256 Enhancing Education Through Technology Act – 20 U.S.C. Sec. 6777 Internet Safety, Children's Internet Protection Act – 47 U.S.C. Sec. 254 Children's Internet Protection Act Certifications, Title 47, Code of Federal Regulations – 47 CFR Sec. 54.520 Joint Operating Committee Policy – 103, 103.1, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 814