Sylvan Heights Science Charter School

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF COMMUNICATIONS AND INFORMATION SYSTEMS (CIS)

ADOPTED: October 20, 2014

	815. ACCEPTABLE USE OF COMMUNICATIONS AND INFORMATION SYSTEMS (CIS)
1. Purpose	The Sylvan Heights Science Charter School ("school") provides employees, students, and Guests ("Users") with hardware, software, and access to the school's Electronic Communication System and network, which includes Internet access, whether wired, wireless, virtual, cloud, or by any other means. The Board supports use of the computers, Internet and other network resources in the school's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration. For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the school as well as the varied instructional needs, learning styles, abilities, and developmental levels of students. The school intends to strictly protect its CIS systems against numerous 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 them. Consequently, Users are required to fully comply with this policy and to immediately report any violations or suspicious activities to the Principal/CAO 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.
2. Definitions 18 U.S.C. Sec. 2256(8) 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254(h)(7)(F)	**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. 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(d) 24 P.S. Sec. 4603	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.
18 U.S.C. Sec. 2256(6) 20 U.S.C. Sec. 6777(e)	**Computer** - includes any school owned, leased or licensed or User-owned personal hardware, software, or other technology used on school premises or at school events, or connected to the school network, containing school programs or school or student data (including images, files, and other information) attached or connected to, installed in, or otherwise used in connection with a Computer. For example, **Computer** includes, but is not limited to, the school and Users': desktop, notebook, powerbook, tablet PC or laptop Computers, printers, facsimile machine, cables, modems, and other peripherals, specialized electronic equipment used for students' special educational purposes, Global Position System (GPS) equipment, RFID, personal digital assistants ("PDAs"), iPods, MP3 players, thumb drives, cell phones (with or without Internet access and/or recording and/or camera/video and other capabilities), telephones, mobile phones or wireless devices, two-way radios/telephones, beepers, paging devices, laser pointers and attachments, Pulse Pens, and any other such technology developed. **Electronic Communications Systems/Electronic Communications** - 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, photooptical or photoelectronic 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, but are not limited to, the internet, intranet, voice mail services, electronic mail services, tweeting, text messaging, instant messages, GPS, PDAs, facsimile machines, cell phones (with or without Internet access and/or electronic mail and/or recording devices, cameras/video, and other capabilities). **Educational Purpose** - includes use of the CIS systems for classroom activities, professional or career development, and to support the school's curriculum, policies,

	regulations, and mission statement.
	Guest - includes, but is not limited to, visitors, workshop attendees, volunteers, adult education staff, students, Board members, independent contractors, and school consultants.
18 U.S.C. Sec. 2252B(d) 20 U.S.C. Sec. 6777(e) 47 U.S.C. Sec. 254(h)(7)(G)	**Harmful to Minors** - under federal law, any picture, image, graphic image file or other visual depictions that: 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.
18 Pa. C.S.A. Sec. 5903(e)(6) 24 P.S. Sec. 4603	Under Pennsylvania law, that quality of 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; 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 Obscene, sexually explicit, Child Pornographic, or other material that is Harmful to Minors, hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, harassing, discriminatory (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, sexting, flagging, terroristic, and advocates the destruction of property.

	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. Personal use must comply with this policy and all other applicable school policies, procedures and rules contained in this policy, as well as Internet service provider ("ISP") terms, local, state and federal laws and must not damage the school's CIS systems.
18 U.S.C. Sec. 2256 20 U.S.C. Sec. 6777(e) 47 U.S.C. Sec. 254(h)(7)(D) 18 Pa. C.S.A. Sec. 5903(e)	**Minor** - for purposes of compliance with the federal Children's Internet Protection Act ("FedCIPA"), 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.
20 U.S.C. Sec. 6777(e) 47 U.S.C. Sec. 254(h)(7)(E)	**Obscene** - Under federal law, analysis of the material meets the following elements: 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.
18 Pa. C.S.A. Sec. 5903(b) 24 P.S. Sec. 4603	Under Pennsylvania law, 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.

18 U.S.C. Sec. 2246 20 U.S.C. Sec. 6777(e) 47 U.S.C. Sec. 254(h)(7)(H) 18 Pa. C.S.A. Sec. 5903(e)(3)	**Sexual Act and Sexual Contact** - is defined at 18 U.S.C. § 2246(2), at 18 U.S.C. § 2246(3), and at 18 Pa. C.S.A. § 5903.
47 U.S.C. Sec. 254(h)(7)(I) 24 P.S. Sec. 4604	**Technology Protection Measure(s)** - specific technology that blocks or filters Internet access to visual depictions that are Obscene, Child Pornography or Harmful to Minors.
18 U.S.C. Sec. 1460(b) 18 Pa. C.S.A. Sec. 2256	**Visual Depictions** - includes undeveloped film and videotape, and data stored on a 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.
3. Authority 47 U.S.C. Sec. 254(1) 24 P.S. Sec. 510, 4604	Access to the school'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 school. The school, further, 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 school will cooperate to the extent legally required with ISP, local, state and federal officials in any investigation concerning or related to the misuse of the CIS systems. 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 access the stored communication of User accounts for any reason in order to uphold this policy, 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, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THE SCHOOL'S CIS SYSTEMS.** The school 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.

20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 24 P.S. Sec. 4604	The school 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 school 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. The Technology Protection Measure must be enforced during use of Computers with Internet access. 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.
20 U.S.C. Sec. 6777(c) 24 P.S. Sec. 4610	Expedited review and resolution of a claim that the 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 Principal/CAO and/or designee. The school has the right, but not the duty, to inspect, review, or retain Electronic Communications created, sent, displayed, received or stored on and over its CIS systems; to monitor, record, check, track, log, access or otherwise inspect; and/or to report all aspects of its CIS systems use. This includes any User's personal Computers, networks, Internet, Electronic Communication systems, databases, files, software, and media that they bring onto school property, or to school events, that were connected to the school network, and/or that contain school programs, or school or Users' data or information, all pursuant to the law, in order to ensure compliance with this policy and other school policies, to protect the school's resources, and to comply with the law. The school 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 support the education of the students. 2. Medium - uses that indirectly benefit the education of the student. 3. Lowest - uses that include reasonable and limited educationally-related employee interpersonal communications and employee limited incidental personal use. 4. Forbidden - all activities in violation of this policy and local, state or federal law.

	The school additionally reserves the right to: 1. Determine which CIS systems services will be provided through school resources. 2. Determine the types of files that may be stored on school file servers and Computers. 3. View and monitor network traffic, fileserver space, processor, and system utilization, and all applications provided through the network and Electronic Communications Systems, including e-mail. 4. Remove excess e-mail 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 when violation of this and any other applicable school policies occur or state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, vendor access, and destruction of school resources and equipment.
4. Delegation of Responsibility	The Principal/CAO and/or designee will serve as the coordinator to oversee the school'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, establish a system to ensure adequate supervision of the CIS systems, maintain executed User acknowledgement/consent forms, and interpret and enforce this policy. The Principal/CAO 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 Records Retention Schedule to include electronically stored information, and establish the school 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 school and school's CIS systems, and to abide by the rules established by the school, its ISP, and local, state and federal laws.

SC 1303.1-A 47 U.S.C. Sec. 254(5)(B) (iii)	The Principal/CAO and/or designee has/have the responsibility to educate minors about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms and cyberbullying awareness and response.
5. Guidelines	Computers, network, Internet, Electronic Communications, information systems, databases, files, software, and media, collectively called "CIS" systems, provide vast, diverse and unique resources. The Board will provide access to the school's CIS systems for Users if there is a specific school related purpose to access information, to research; to collaborate, to facilitate learning and teaching; and to foster the educational purpose and mission of the school. For Users, the school's CIS systems must be used for education related purposes and performance of school job duties in compliance with this policy. For employees, Incidental Personal Use of school Computers is permitted as defined in this policy but they should have no expectation of privacy in anything they create, store, send, receive, or display on or over the school'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 Computers which are located or installed on school property or which have been brought onto a school location by an employee or student. For personal technology devices brought onto the school property, to school events, or connected to the school 's network and systems, if the school reasonably believes the Computer and/or personal technology devices contain school information or contain information that violates a school policy, the legal rights of the school or another person, involves significant harm to the school or another person, or involves a criminal activity, they may be legally accessed to ensure compliance with this policy, other school policies, and federal and state law. Users may not use their personal Computers and personal technology devices to access the school's intranet, Internet or any other CIS system unless approved by the Principal/CAO and/or designee. Due to the nature of the Internet as a global network connecting thousands of Computers around the world, Inappropriate Matter can be accessed through the network and electronic systems. Because of the nature of the technology that allows the Internet to operate, the school cannot completely block access to these resources. Accessing these and similar types of resources may be considered an

	unacceptable use of school 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 school policies. The school must publish a current version of this policy on its web site so that all Users are informed of their responsibilities. A copy of this policy and applicable acknowledgement/consent form(s) must be provided to all Users, who must sign such form(s), either by electronic or written means. Employees must be capable and able to use the school's CIS systems and software relevant to the employee's responsibilities. Users must practice proper etiquette and school ethics, must agree to the requirements of this policy, and are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:
Pol. 218	1. Be polite and do not become abrasive in messages to others. General school rules, regulations and policies for behavior and communicating apply. 2. Use appropriate language and do not swear or use vulgarities or other inappropriate language. 3. Do not reveal the personal addresses or telephone numbers of others. 4. Recognize that e-mail is not private or confidential. 5. Do not use the Internet or e-mail in any way that would interfere with or disrupt its use by other Users. 6. Consider all communications and information accessible via the school's Internet provider to be the property of the school. 7. Respect the rights of other Users to an open and hospitable technology environment, regardless of race, sexual orientation, color, religion, national origin, gender, creed, ethnicity, age, marital status, political beliefs, or disability status. <u>Access To The CIS Systems</u> Users' CIS systems accounts must be used only by authorized owners of the accounts and only for authorized purposes.

An account must be made available according to a procedure developed by appropriate school authorities.

This policy, as well as other relevant school policies, rules, regulations and administrative regulations, will govern use of the school's CIS systems for Users.

Types of services that could be accessed through the school 's CIS systems include, but are not limited to:

1. World Wide Web - School employees, students, and Guests will have access to the World Wide Web through the school's CIS systems, as needed.

2. E-Mail - School employees may be assigned individual e-mail accounts for work related use, as needed. Students may be assigned individual e-mail accounts, as necessary, by the Principal/CAO and/or designee at the recommendation of the teacher who will also supervise the students' use of the e-mail service.

3. Guest Accounts - Guests may receive an individual web account with the approval of the Principal/CAO and/or designee if there is a specific school related purpose requiring such access. Use of the CIS systems by a Guest must be specifically limited to the school related purpose and comply with this policy and all other school policies, procedures, regulations and rules, as well as ISP terms, local, state and federal laws, and may not damage the school 's CIS systems. An applicable acknowledgment/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 or electronic signature is required.

4. Blogs - Employees may be permitted to have school sponsored blogs after they receive training and the approval of the Principal/CAO and/or designee. All bloggers must follow the rules provided in this policy and other applicable policies, regulations and rules of the school.

5. Web 2.0 Second Generation And Web 3.0 Third Generation Web-Based Services - Certain school authorized Second Generation and Third Generation Web-based services, such as blogging, authorized social networking sites, wikis, podcasts, RSS feeds, social software, folksonomies, and interactive 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 school; however, such use must be approved by the Principal/CAO and/or designee followed by training authorized by the school. Users must comply with this policy as well as any other relevant policy, rules or regulations (including the copyright, participatory

learning/collaborative/social networking regulations, and rules during such use).

Parental Notification And Responsibility

The school will notify the parents/guardians about the school's CIS systems and the policies governing their use. This policy contains restrictions on accessing Inappropriate Matter. 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 school to monitor and enforce wide range of social values in student use of the Internet. Further, the school recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children. The school will encourage parents/guardians to specify to their children what material is and is not acceptable for their children to access through the school's CIS system.

School Limitation Of Liability

The school makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the school's CIS systems will be error-free or without defect. The school does not warrant the effectiveness of Internet filtering. The electronic information available to Users does not imply endorsement of the content by the school. Nor is the school responsible for the accuracy or quality of the information obtained through or stored on the CIS systems. The school 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 CIS systems. The school will not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The school will not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the school's CIS systems. In no event will the school be liable to the User for any damages whether direct, indirect, special or consequential, arising out of the use of the CIS systems.

Prohibitions

The use of the school'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 school 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 school resources are accessed whether on school property, at school events, connected to the school's network, when using mobile commuting equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when an employee or student uses their own equipment.

	A. *General Prohibitions* Users are <u>prohibited</u> from using school CIS systems to: 1. Communicate about nonwork or nonschool related communications unless the employees' use comports with this policy's definition of Incidental Personal Use. 2. Send, receive, view, upload, download, store, access, print, distribute, or transmit material that is Harmful to Minors, indecent, Obscene, pornographic, Child Pornographic, terroristic, including but 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, e-mailing, texting, among others). Neither may Users advocate the destruction of property. 3. Send, receive, view, upload, download, store, access, print, distribute, or transmit Inappropriate Matter and material likely to be offensive or objectionable to recipients.
SC 13-1301.1-A	4. Cyberbullying another individual or entity. 5. Access or transmit gambling 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, profane, or inflammatory communications. 8. Participate in unauthorized Internet Relay Chats, instant messaging communications and Internet voice communications (on-line; real-time conversations) that are not for school-related purposes or required for employees to perform their job duties. Students must obtain consent from their teacher to use IRC's, however they may not use instant messaging or text messaging. Employees may only use instant messaging if consent was obtained from the Principal/CAO and/or designee. 9. Facilitate any illegal activity. 10. Communicate through e-mail for noneducational purposes or activities,

unless it is for Incidental Personal Use as defined in this policy. The use of e-mail to mass mail noneducational or nonwork related information is expressly prohibited (for example, the use of the everyone distribution list, building level distribution lists, or other e-mail distribution 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 school policies); conduct unauthorized fundraising or advertising on behalf of the school and non-school organizations; resale of school Computer resources to individuals or organizations; or use the school's name in any unauthorized manner that would reflect negatively on the school, its employees, or students. **Commercial purposes** are defined as offering or providing goods or services or purchasing goods or services for personal use. School acquisition policies must be followed for school purchase of goods or supplies through the school system.

12. Engage in political lobbying.

13. Install, distribute, reproduce or use unauthorized copyrighted software on school Computers, or copy school software to unauthorized Computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright.

14. Install Computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on school Computers is restricted to the Principal/CAO and/or designee.

15. Encrypt messages using encryption software that is not authorized by the school from any access point on school equipment or school property. Users must use school approved encryption to protect the confidentiality of sensitive or critical information in the school's approved manner.

16. Access, interfere, possess, or distribute confidential or private information without permission of the school'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 school information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the school's business or educational interest.

19. Send unsolicited commercial electronic mail messages, also known as "spam".

20. Post personal or professional web pages without administrative approval.

21. Post anonymous messages.

22. Use the name of the Sylvan Heights Science Charter School in any form in blogs, on school Internet pages or web sites not owned or related to the school, or in forums/discussion boards, and social networking web sites, to express or imply the position of the school without the expressed, written permission of the Principal/CAO and/or designee. When such permission is granted, the posting must state that the statement does not represent the position of the school.

23. Bypass or attempt to bypass Internet filtering software by any method including, but not limited to, the use of anonymizer/proxies or any web sites that mask 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 and/or obtain personal information under false pretenses with the intent to defraud another person.

26. Use location devices to harm another person.

B. Access and Security Prohibitions

Users must immediately notify the Principal/CAO and/or designee if they have identified a possible security problem. Users must read, understand, and submit an electronically or written signed acknowledgement form(s), and comply with this policy that includes network, Internet usage, Electronic Communications, telecommunications, nondisclosure, and physical and information security requirements. The following activities related to access to the school 's CIS systems, and information are prohibited:

1. Misrepresentation (including forgery) of the identity of a sender or source of communication.

2. Users are required to use unique strong passwords that comply with the

school's password, authentication and syntax requirements. Users must not acquire or attempt to acquire User ID and passwords of another. Users will be held responsible for the result of any misuse of Users' names or passwords while the Users' systems access were left unattended and accessible to others, whether intentional or, whether 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 school resources to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons, such as 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 school 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 school.

8. Accessing any web site that the school has filtered or blocked as unauthorized. Examples include, but are not limited to, unauthorized social networking, music download, and gaming sites.

9. Users must protect and secure all electronic resources and information data and records of the school from theft and inadvertent disclosure to unauthorized individuals or entities when they are under the supervision and control of the school and when they are not under supervision and control of the school, for example, but not limited to, working at home, on vacation or elsewhere. If any User becomes aware of the release of school information, data or records, the release must be reported to the Principal/CAO and/or designee, immediately.

C. *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, and other program code, the sending of electronic

chain mail, distasteful jokes, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts. The User may not hack or crack the network or others' Computers, whether by parasiteware or spyware designed to steal information, or viruses and worms or other hardware or software designed to damage the CIS systems, or any component of the network, or strip or harvest information, or completely take over a person's Computer, or to "look around."

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 school 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, or by other means.

6. Connecting unauthorized hardware and devices to the CIS systems.

7. Loading, downloading, or use of unauthorized games, programs, files, or other electronic media, including, but not limited to, downloading music files.

8. Intentionally damaging or destroying the integrity of the school's electronic information.

9. Intentionally destroying the school's Computer hardware or software.

10. Intentionally disrupting the use of the CIS systems.

11. Damaging the school's CIS systems, networking equipment through the Users' negligence or deliberate act, including, but not limited to vandalism.

12. Failing to comply with requests from school staff to discontinue activities that threaten the operation or integrity of the CIS systems.

<u>Content Guidelines</u>

Information electronically published on the school '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 student's date of birth, Social Security number, driver's license number, financial information, credit card number, health information, phone numbers, street address, or box number, name, (other than first name), or the names of other family members without parental consent.

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 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 school policies and guidelines.

5. Documents to be published on the Internet must be edited and approved by the Principal/CAO or designee before publication.

Due Process

The school will cooperate with the ISP rules and local, state, and federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through the school'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 school may terminate account privileges by providing notice to the User.

Search And Seizure

Users' violations of this policy, any other school policy, or the law may be discovered by routine maintenance and monitoring of the school CIS system, or any method stated in this policy, or pursuant to any legal means.

The school reserves the right, but not the duty, to inspect, review, or retain Electronic Communications created, sent, displayed, received, or stored on and over

	its CIS systems; to monitor, record, check, track, log, access or otherwise inspect; and/or report all aspects of its CIS systems. This includes any personal Computers, network, Internet, Electronic Communication systems, databases, files, software, and media that they bring onto school property, or school events, that were connected to the school's network, and/or that contain school programs, or school or Users' data or information, all pursuant to law, in order to ensure compliance with this policy and other school policies, to protect the school 's resources, and to comply with the law. Everything that Users place in their personal files should be written as if a third party will review it. <u>Copyright Infringement And Plagiarism</u>
17 U.S.C. Sec. 101 et seq Pol. 814	Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through school resources. Users will 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. Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing the law. The school does not permit illegal acts pertaining to the copyright law. Therefore, any Users violating the copyright law does so at their own risk and assume all liability. Violations of copyright law include, but are not limited to, the making of 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, and deep-linking and framing into the content of others' web sites. Further, the illegal installation of copyrighted software or files for use on the school's Computers is expressly prohibited. This includes all forms of licensed software — shrink wrap, click wrap, browse wrap, and electronic software, downloaded from the Internet.
17 U.S.C. Sec. 1202 Pol. 814	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. Users must not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices. <u>Selection Of Material</u>

	School policies on the selection of materials will govern use of the school's CIS systems. When using the Internet for class activities, teachers must 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 web sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the web site. Teachers must provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers must 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. <u>School Web Site</u> The school has established and maintains a web site and will develop and modify its web pages that will present information about the school under the direction of the Principal/CAO, and/or designee.
17 U.S.C. Sec. 512	The school may limit its liability by complying with the Digital Millennium Copyright Act's safe harbor notice and takedown provisions. <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 school personal and private information/data, images and copyrighted material in their blog, and may not disrupt the school. Conduct otherwise will result in actions further described in the *Consequences for Inappropriate, Unauthorized and Illegal Use* section of this policy and provided in other relevant school policies. <u>Safety And Privacy</u>
47 U.S.C. Sec. 254	To the extent legally required, Users of the school's CIS systems will be protected from harassment or commercially unsolicited Electronic Communication. Any User who receives threatening or unwelcomed communications must immediately send or take them to the Principal/CAO 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 any way, may not use spyware, cookies, or use school or personnel employee technology or resources in any way to invade one's privacy. Additionally, Users may not disclose, use or disseminate confidential and personal information about students or employees by 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, and resumes or other information relevant to seeking employment at the school by using a PDA, iPhone, Blackberry, cell phone (with or without camera/video) and/or other Computer, unless legitimately authorized to do so. If the school requires that data and information be encrypted Users must use school authorized encryption to protect their security. Student Users must agree not to meet with someone they have met online unless they have parental consent. <u>Consequences For Inappropriate, Unauthorized And Illegal Use</u>
Pol. 417, 98-205 (Student Code of Conduct)	General rules for behavior, ethics, and communications apply when using the CIS systems and information, in addition to the stipulations of this policy. Users must be aware that violations of this policy or other policies, 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 for employees), dismissal, expulsions, and/or legal proceedings on a case-by-case basis. This policy incorporates all other relevant school policies, such as, but not limited to, the student and professional employee discipline policies, applicable Code of Student Conduct, copyright, property, curriculum, terroristic threat, vendor access, and harassment policies. Users are responsible for damages to the network, equipment, Electronic Communications systems, and software resulting from negligent, deliberate, and willful acts. Users will also be responsible for incidental or unintended damage resulting from willful or deliberate violations of this policy. For example, Users will be responsible for payments related to lost or stolen Computers and/or school equipment, and recovery and/or breach of the data contained on them. Violations as described in this policy may be reported to the school, appropriate legal authorities, whether the ISP, local, state, or federal law enforcement and may constitute a crime under state and/or federal law, which may result in arrest, criminal prosecution, and lifetime inclusion on a sexual offenders registry. The school will

	cooperate to the extent legally required with authorities in all such investigations. Vandalism will result in cancellation of access to the school's CIS systems and resources and is subject to discipline. Any and all costs incurred by the school for repairs and/or replacement of software, hardware and data files and for technological consultant services due to any violation of this policy, or federal, state, or local law, shall be paid by the User who caused the loss. References: School Code – 24 P.S. Sec. 510, 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 Abuse – 18 U.S.C. Sec. 2246 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 – 47 U.S.C. Sec. 254 Children's Internet Protection Act Certifications, Title 47, Code of Federal Regulations – 47 CFR Sec. 54.520 Board Policy – 417