OLD FORGE SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF TECHNOLOGY AND THE INTERNET

ADOPTED: May 15, 2002

REVISED: April 13, 2011

815. ACCEPTABLE USE OF TECHNOLOGY AND THE INTERNET

1. Purpose

The Board supports use by employees and students of the Internet and other computer networks in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration.

Access to the district's network shall be for specific district-related purposes to access information and research; to collaborate; to facilitate learning and teaching; and to foster the educational mission, vision, and beliefs of the school district.

The district provides students, staff and other authorized individuals with access to the district's computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means. The district provides wired and/or wireless Internet access to any and all school owned device. This device should be school owned since it would then be a part of the district's domain and will have restricted access to objectionable sites through district filtering and will also have appropriate anti-virus software.

2. Authority
20 U.S.C. Sec. 6777
47 U.S.C. Sec. 254

The electronic information available to students and staff does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged, or unavailable when using the network or for any information that is retrieved via the Internet. The district operates and enforces technology protection measures that filter online activities of all users so as to filter or block inappropriate matter on the Internet.

The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.

It is often necessary to access Users' accounts in order to perform routine maintenance and security tasks. System administrators have the right to access by interception, and the right to access the stored communication of Users' accounts for any reason in order to uphold and enforce this policy and other school district policies, regulations, rules, procedures, the law, and to maintain the system. Users of the school district's CIS systems who transmit or receive communications and

	information shall be deemed to have consented to having the content of any such communications recorded, checked, received, monitored, tracked, logged, accessed and otherwise inspected or used by the school district, and to the school district monitoring and allocating fileserve space. Passwords and message delete functions do not restrict the school district's ability or right to access such communications or information. Users have no privacy expectations in the contents of their personal files or any of their use of the district's network. The district reserves the right to monitor, track and/or log user access, as well as monitor and allocate fileserver space and access all user files. The Board establishes that **computer and** network use is a privilege, not a right; inappropriate, unauthorized, and illegal use will result in cancellation of those privileges and appropriate disciplinary action. The district will cooperate to the extent legally required with Internet Service Provider (ISP), local, state, and federal officials in any investigation concerning or related to the misuse of the district's **Internet, computers and** network **resources**. **The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.**
3. Definitions 18 U.S.C. Sec. 2256	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. 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	Under Pennsylvania law, 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. Child pornography found on an employee's computer will be reported to the police.
Pol. 237	Computer - includes any district-owned, leased or licensed or user-owned personal hardware, software, or other technology used on district premises or at district events, or connected to the district network, containing district programs or school district or student data including images, files, and other information attached or connected to, installed in, or otherwise used in connection with a computer. Computer includes, but is

	not limited to desktop; notebook; power book; tablet PC, **iPad, Kindle** or laptop computers; printers; cables; modems and other peripherals, including thumb and flash drives; specialized electronic equipment used for students' special educational purposes; global positioning system (GPS) equipment; personal digital assistants (PDAs); cell phones, with or without Internet access and/or recording and/or camera/video and other capabilities; mobile phones, or wireless devices; two-way radios/telephones; beepers; paging devices; laser pointers and attachments; and any other such technology developed.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	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. 3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value as to minors.
18 Pa. C.S.A. Sec. 5903	Under Pennsylvania law, 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. 3. Taken as a whole, lacks serious literary, artistic, political, educational or scientific value for minors.
47 U.S.C. Sec. 254	Minor - for purposes of compliance with the Children's Internet Protection Act (CIPA), an individual who has not yet attained the age of seventeen (17). For other purposes, minor shall mean the age of minority as defined in the relevant law. Network - a system that links two (2) or more computer systems, including all components necessary to effect the operation, including, but not limited to: computers, copper and fiber cabling, wireless communications and links, equipment closets and enclosures, network electronics, telephone lines, printers and other peripherals including thumb and flash drives, storage media, software, and other computers and/or networks to which the network may be connected, such as the Internet or those of other institutions. 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. 3. Whether the work taken as a whole lacks serious literary, artistic, political, educational, or scientific value.
18 Pa. C.S.A Sec. 5903	Under Pennsylvania law, analysis of the material meets the following elements: 1. The average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest. 2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene. 3. The subject matter, taken as a whole lacks serious literary, artistic, political, educational or scientific value. Proxy Server - a server that can be used to control and speed up access to the Internet. It can also allow multiple computers in a network to access the Internet by using a single IP address.
18 U.S.C. Sec. 2246 18 Pa. C.S.A Sec. 5903	Sexual Act and Sexual Contact - as defined at 18 U.S.C. Sec. 2246, and at 18 Pa. C.S.A. Sec. 5903.
47 U.S.C. Sec. 254	Technology Protection Measure(s) - a 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. 2256	Visual Depictions - undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image but does not include mere words.
4. Delegation of Responsibility	The district shall make every effort to ensure that this resource is used responsibly by students and staff. These resources may include, but are not limited to, network user accounts, computers, the Internet, e-mail, blogs, social networking web sites and other second-generation web services. **Users of district networks or district-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the district uses monitoring**

	systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen information. Student user agreements shall also be signed by a parent/guardian. Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals. Students and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet. The building administrator shall have the authority to determine what inappropriate use is. The building administrator shall notify the Superintendent when issues outside the guidelines are encountered.
47 U.S.C. Sec. 254	The technology specialist or designee shall be responsible for implementing technology and procedures to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to: 1. Utilizing a technology protection measure that blocks of 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 Board. 2. Maintaining and securing a usage log. 3. Monitoring online activities of minors. 4. Establishing a process for setting up user accounts, establishing quotas for fileserver storage space, establishing a document and e-mail retention procedure, as well as a virus protection process.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	The district 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 district operates and enforces technology protection measure(s) that block or filter online activities of minors or its computers used and accessible to adults and students so as to filter or block inappropriate matter on the Internet. **The technology protection measure shall be enforced during use of computers with Internet access. Upon request by students or staff, the Superintendent 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. Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review. Inappropriate matter includes, but is not limited to visual, graphic, text and any other form of obscene, sexually explicit, child pornographic, or other material that is harmful to minors, or that are 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; terroristic; and advocates the destruction of property. Measures designed to restrict adults' or minors' access to material harmful to minors may be disabled to enable an adult or student 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. 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 a written consent from a parent/guardian for a student, and upon the written request from an employee.
47 U.S.C. Sec. 254 Pol. 249	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 network resources. This includes educating minors about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms and cyberbullying awareness and response. All users have the responsibility to respect the rights of all other users within the school district and to abide by the rules established by the school district, local, state and federal laws. The school district will notify parents/guardians annually about the network systems and the policies governing their use. A copy of this policy shall be posted on the district's web site, published in the annual student handbook, and available directly from the Office of the Superintendent.
5. Guidelines	**<u>Access to the CIS Systems</u>** **a. Users' CIS systems accounts must be used only by authorized owners of the accounts and only for authorized purposes.** **b. An account will be made available to individual users according to a procedure to be developed by appropriate School District authorities.** **c. CIS System**. • **This Policy, as well as other relevant school district policies, regulations, rules and procedures will govern use of the**

school district's CIS systems for Users.

d. Types of Services include, but are not limited to:

- **Internet - School district employees, students, and guests will have access to the internet through the school district's CIS systems, as needed.**
- **E-Mail - School district 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 Director of Technology and/or designees, and at the recommendation of the Principal.**
- **Blogs - Employees may be permitted to have school district-sponsored blogs after having received training and the approval of the Director of Technology and/or designees, and at the recommendation of the Principal. All bloggers must follow the rules provided in this policy and other applicable policies, regulations, rules and procedures of the school district.**
- **Web2.0 Second Generation and Web 3.0 Third Generation Web-based Services - Certain school district authorized Second Generation and Third Generation Web-based services, such as blogging, wikis, podcasts, RSS feeds, social software, and interactive collaboration tools that emphasize online participatory learning (where Users share ideas, comment on one others' 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 district; however, such use must be approved by the Director of Technology and/or designees, followed by training authorized by the school district, and at the recommendation of the Principal. Users must comply with this policy as well as any other relevant policies, regulations, rules and procedures, including copyright, participatory learning/collaborative/social networking during such use.**

<u>Parental Notification And Responsibility</u>

The district will notify the parents/guardians about the district's CIS systems and the policies governing their use. This policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the school district to monitor and enforce a wide range of social values in student use of the Internet. Further, the school district recognizes that the parents/guardians bear primary responsibility for transmitting their particular set of family values to their children The district will encourage parents/guardians to specify to

their children what material is and is not acceptable for their children to access through the district's CIS systems **prior to the start of school.**

School District Limitation Of Liability

The district makes no warranties of any kind; either expressed or implied that the functions or the services provided by or through the district's CIS systems will be error-free or without defect. The district does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the school district. The district is neither responsible for nor guarantees the accuracy or quality of the information obtained through or stored on the CIS systems. The district 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 district shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The district shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the district's CIS systems. In no event shall the school district be liable to the user for any damages whether direct, indirect, special or consequential, arising out of the use of the CIS systems.

Network accounts shall be used only by the authorized owner of the account for its approved purpose. Network users shall respect the privacy of other users on the system.

Prohibitions

Students and staff are expected to act in a responsible, ethical, and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Illegal activity.
2. Commercial or for-profit purposes.
3. Non-work or non-school related work.
4. Product advertisement or political lobbying.
5. Bullying/Cyberbullying or other type of harassment prohibited by law, the Student Code of Conduct or Board policy.
6. Hate mail, discriminatory remarks, and offensive or inflammatory communication (relay chat, news groups, e-mail, blogs, social networking sites, etc.).

	7. Unauthorized or illegal installation, distribution, reproduction or use of copyrighted materials. 8. Access to materials, images or photographs that are obscene or pornographic, lewd or otherwise illegal or child pornography. 9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy. 10. Use of inappropriate language or profanity. 11. Transmission of material likely to be offensive or objectionable to recipients. 12. Intentional obtaining or modifying of files, passwords and data belonging to other users. 13. Impersonation of another user, anonymity and pseudonyms. 14. Fraudulent copying, communications, or modification of materials in violation of copyright laws. 15. Loading or using of unauthorized games, programs, files, or other electronic media. 16. Disruption of the work of other users. 17. Destruction, modification, abuse, or unauthorized access to network hardware, software and files. 18. Quoting, summarization or other recounting of personal communications in a public forum without the original author's prior consent. 19. Communication of private/personal information of others. 20. The purchase or sale of any product or service. 21. Participation in online auctions or online gaming and/or gambling. 22. Use of the school's name, logos and web material in personal communications. 23. Any suggestion that the employee or student represents the school in online activities.

	24. Employee/Student communications considered to be boundary invasions. 25. **Accessing the Internet, district computers or other network resources without authorization.** 26. **Disabling or bypassing the Internet blocking/filtering software without authorization.** 27. **Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.** 28. **The district shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the district website, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.** <u>Consequences For Inappropriate Use</u> The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Illegal use of the network, intentional deletion or damage to files of data belonging to others, copyright violations, and theft of services will be reported to the appropriate legal authorities for possible prosecution. General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use. Vandalism will result in cancellation of access privileges**, disciplinary action and/or legal proceedings. Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses. **Failure to comply with this policy or inappropriate use of the Internet, district network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings.** <u>Copyright</u>
Pol. 814	The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded or downloaded from the network shall be subject to fair use guidelines **and applicable laws and regulations.**

	School district guidelines on plagiarism, as well as the Student Code of Conduct, will govern use of material accessed through the district network. The district's guidelines on plagiarism can be found in the student handbook. **<u>District Website</u>** **The district shall establish and maintain a website and shall develop and modify its web pages to present information about the district under the direction of the Superintendent or designee. All users publishing content on the district website shall comply with this and other applicable district policies.** **Users shall not copy or download information from the district website and disseminate such information on unauthorized web pages without authorization from the Superintendent.** <u>Safety</u> To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications 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, e-mail, Internet, etc.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.
47 U.S.C. Sec. 254	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. <u>Security</u>

	System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, the following guidelines shall be followed: 1. Employees and students shall not reveal their passwords to another individual. 2. Users are not to use a computer that has been logged in under another student's or employee's name. If a previous user has not logged off, the current user must immediately log out and then log back in under his/her own name and password. 3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network. 4. Users must create passwords that follow the guidelines for required syntax. 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 – 28 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 – 218, 237, 248, 249, 814