

	<p>filtering or site categorization.</p> <p>The District shall not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored in any IT resources. The District shall not be responsible for financial obligations arising from the unauthorized use of IT resources. In no event shall the District be liable to the user for any damages whether direct, indirect, special or consequential, arising out of the use of the District IT resources.</p> <p>Personal computer technology or IT resources brought onto District property or at District events, or connected to the District's network, that the District reasonably believes contain District information or contain information that violates a District Policy, or contain information/data that the District reasonably believes involves a criminal activity may be legally accessed to ensure compliance with Board Policy and local, state, federal or international law. Users may not use their personal computer technology or IT resources connected to the District's electronic communications systems unless approved, in advance, by the Director of Technology or designee and/or authorized as part of the District's services for users.</p> <p>The District reserves the right, though it has no duty, to monitor, track, log, access and or record all aspects of IT resource use, pursuant to law, to determine whether or not the resources are being used for educational or administrative value or to ensure compliance with Board Policy. The District also reserves the right to view and monitor network traffic, file server space, processor and system utilization, and all applications provided through the IT resources and electronic communications systems, including e-mail and other electronic communications.</p> <p>By using District IT resources, the user consents to routine monitoring and maintenance by District technology staff or contracted service providers performed in the ordinary course of business to maintain the security and integrity of the resources. Monitoring may include tracking a user's IT resource use and/or reading, listening to, or otherwise observing the user's wire, oral or electronic communications. In addition, backup files may be maintained for archiving purposes and may contain copies of all user files, records and communications.</p> <p>Users have no privacy expectation for the contents of their files or any of their use of the District's IT resources. This routine maintenance and monitoring is necessary and may lead to discovery that a user has or is violating Board Policy or state, federal and/or international law. If a problem is discovered, an individual search will be conducted when there is a reasonable suspicion that the user has violated the state, federal and/or international and/or Board Policy. The nature of the search/investigation will be reasonable and in keeping with the nature of the alleged misconduct. While monitoring IT resources, the District reserves the right to restrict and allocate file storage space, determine the types of files that may be stored on</p>
--	--

<p>3. Definitions</p>	<p>District IT resources, and remove excess e-mail or files utilizing an inordinate amount of storage space or which have not been accessed for an extended period of time.</p> <p>The Board establishes that access to and use of IT resources is a privilege, not a right. IT resources, as well as the user accounts and information are the property of the District. Inappropriate, unauthorized and illegal use may result in restriction, suspension or cancellation of those privileges and appropriate legal or disciplinary action up to and including student expulsion, staff dismissal, and/or referral for prosecution. In order to prevent unauthorized, inappropriate or illegal activity, the District reserves the right to deny user access to IT resources.</p> <p>The District shall cooperate to the extent legally required with service provider(s) and governmental officials in any investigation concerning or relating to any misuse or illegal activities conducted utilizing District IT resources. District employees should be aware that their personal files may be subject to public access and/or discoverable under state or federal law.</p> <p>The Administration is authorized to implement this Policy by appropriate administrative regulations. Such regulations shall comply with all applicable international, federal, state, and local laws and regulations, as may be amended from time to time, related to child safety and privacy, including but not limited to, the Children’s Internet Protection Act of 2000 (P.L. 106-543), the Children’s Online Privacy Protection Act of 1998 (15 U.S.C.§6501 et seq.), the Family Educational Rights and Privacy Act (20 U.S.C.§1232(g)), and the Electronic Communications Privacy Act (18 U.S.C. §2510 et seq.).</p> <p>The protection of District IT resources from either internal or external exposure is the responsibility of the IT Department. However, users are responsible for helping to ensure the protection of IT resources through their responsible use of said resources, as well as reporting any violations of Board Policy or suspicious activities. Students and building-level staff should report this to the building principal or in the absence of the principal or designee, the Director of Technology. Reports should be made by central office staff to the Director of Technology. Failure to report known violations or suspicious activity will result in action defined by this and/or other relevant Board Policy.</p> <p>Active user – an individual in control of and using an IT resource. Active users are responsible for their actions when using IT resources.</p> <p>Blog – short for weblog, it is a personal online journal that is frequently updated and intended for general public consumption. Blogs are defined by their format: a series of entries posted to a single page in reverse-chronological order. Blogs generally represent the personality of the author or reflect the purpose of the Web site that hosts the blog.</p>
-----------------------	--

<p>18 U.S.C. 2256(8)</p> <p>PA C.S. 6312</p>	<p>Browser – a software application that enables a user to display and interact with text, images, and other information typically located on a web page at a website on the World Wide Web or a local area network. Text and images on a web page can contain hyperlinks to other web pages at the same or different websites. Web browsers allow a user to quickly and easily access information provided on many web pages at many websites by traversing these links.</p> <p>Casting – the preparation and distribution of audio and/or other media files for download to digital music or multimedia players. Also known as “podcasting”.</p> <p>Child Pornography – under Federal law, any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; 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 such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.</p> <p>Child Pornography – under Pennsylvania law, any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of 18 years engaging in a prohibited sexual act or in the simulation of such act.</p> <p>Commercial purposes – offering or providing goods or services or purchasing goods or services for personal use. Board Policy regarding acquisition and purchasing shall be followed for District purchase of goods or services through IT resources and/or electronic communications systems.</p> <p>Computer – a device that accepts information in the form of digitized data and can manipulate it for some result based on a program or predetermined set of instructions on how the data is to be processed. Devices include 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 applications or District or student data (including images, files and other information) attached or connected to, installed in, or otherwise used in connection with a computer. Examples include, but are not limited to, desktop, notebook, laptop or tablet computer, printer, personal digital assistant (PDA), specialized electronic equipment used for students’ special educational purposes, Global Positioning System (GPS) equipment, FAX machine, MP3 (or other audio format) player, telephone, cellular or wireless phone, wireless devices, two-way radio/telephone, beeper, paging device, laser pointer and attachments, and any other such technology developed.</p>
--	---

	<p>Cookies – messages that may include personally identifiable information, which are typically stored in a text file and used to identify visitors to web sites and possibly prepare customized web pages for them.</p> <p>Copyright infringement – occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user must follow the expressed requirement. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner. More information can be found in the Policy on copyrighted material. (Policy #814)</p> <p>Cracking – the act of attempting to discover another user’s password or authorization information.</p> <p>Discussion board – a discussion board (known also by various other names such as discussion group, discussion forum, message board, and online forum) is a general term for any online "bulletin board" where you can leave and expect to see responses to messages you have left. Or you can just read the board. On the Internet, Usenet provides thousands of discussion boards; these can be viewed from a browser or specialized software.</p> <p>DoS attack – a denial of service attack is designed to overload an information technology resource and deprive users of its full functionality.</p> <p>Due process – Due process is a legal concept that ensures entities will respect all of a person's legal rights in order to guarantee fundamental fairness, justice, and liberty.</p> <p>Educational use – use of IT resources for specific, curriculum-related classroom activities preapproved by the instructor or administration. Also includes professional or career development activities and activities in support of the District’s policies and mission statement.</p> <p>Electronic communications – any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic, or photo-optical system via an information technology resource. Examples include, but are not limited to, electronic mail services, voice mail services, GPS.</p> <p>Electronic communications systems – 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 designated as a system for electronic communications or is implicitly used for such purposes.</p>
--	--

	<p>Electronic security incident – electronic activities that result in the damage to or misuse of the IT resources of the District.</p> <p>E-mail – the exchange of computer-stored messages via a communications channel.</p> <p>E-Rate – a program administered by the Universal Service Administrative Company (USAC) under the direction of the Federal Communications Commission (FCC) that provides discounts to assist schools and libraries in the United States to obtain affordable telecommunications and Internet access.</p> <p>FERPA – The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.</p> <p>File Transfer Protocol (FTP) – a protocol used for downloading files.</p> <p>Filtering – a filter is software or a hardware device that can screen an incoming electronic communication to determine whether some or all of it should not be displayed to the user. The filter checks the origin or content of the electronic communication against a set of rules to determine if it should be displayed or not.</p> <p>Firewall – hardware or software that controls and manages the connections allowed to networks or IT resources that it protects.</p> <p>Guest user – any person accessing District IT resources who is not a student or staff member. This includes, but is not limited to, visitors, volunteers, independent contractors and vendors. Accounts will be issued to guests only if there is a specific District-related purpose requiring such access.</p> <p>Hacking – the activity of unauthorized use or attempts to access IT resources (regardless of intent to cause harm) including, but not limited to, attempts to circumvent or bypass security mechanisms.</p> <p>Harassment – utilizing information technology resources and/or electronic communications systems in a course of conduct directed at a specific person or group of persons that causes substantial emotional distress and serves no legitimate purpose. If a user is told by a person to stop doing something, they must stop.</p> <p>Hardware - in information technology, hardware is the physical aspect of computers, telecommunications, and other information technology resources and/or electronic communications devices.</p> <p>Harmful to Minors – as defined at 20 U.S.C. § 6801 and 47 U.S.C. § 254(h)</p>
--	---

	<p>Harmful to Minors – as defined at 18 PA C.S. § 5903(e)(6)</p> <p>HIPAA – HIPAA is the United States Health Insurance Portability and Accountability Act of 1996. Among other things, the Act mandates security mechanisms to ensure confidentiality and data integrity for any information that identifies an individual.</p> <p>Inappropriate material – material that does not serve an instructional or educational purpose and that: (i) is profane, vulgar, lewd, obscene, offensive, indecent, sexually explicit, or threatening; (ii) advocate illegal or dangerous acts; (iii) causes disruption to the District, its employees, or students; (iv) advocates violence; or (v) contains knowingly false, recklessly false, or defamatory information.</p> <p>Incidental personal use – use of IT resources by staff for nonwork, noneducational reasons. Authorized only so long as the District incurs no cost from that use, the use does not result in loss of employee productivity and does not interfere with official duties and responsibilities, and does not preempt any legitimate activity of the District. Employees have no inherent right to employ IT resources for personal use. Any educational purpose will take precedence over all incidental personal use. Incidental personal use will be measured in time (minimal time and duration) and frequency (occasional use). Incidental personal use must not result in financial gain for the user or be for business purposes where the business is owned by the employee or the work is done for another business.</p> <p>Information Technology Resource – any computer, personal digital assistant (PDA), networking device, telephone, cellular or wireless phone (with or without Internet access and/or electronic mail), recording devices, video or still cameras, copier, printer, FAX machine, peripheral or other electronic technology which is owned by the District or is licensed/leased by the District. In addition, any information technology which connects directly or indirectly to the District data or telephone networks, uses District network resources, connects directly or indirectly to another IT resource or other device owned or operated by the District, and/or otherwise uses or affects District information technology facilities is subject to District information technology policies, no matter who owns it.</p> <p>Instant messaging – instant messaging (sometimes called IM or IMing) is the ability to easily see whether a chosen friend or co-worker is connected to a network and, if they are, to exchange messages with them. Instant messaging differs from ordinary e-mail in the immediacy of the message exchange and also makes a continued exchange simpler than sending e-mail back and forth. Most exchanges are text-only. However, some services allow voice messaging and file sharing and other collaboration tools.</p> <p>Internet – a worldwide system of computer networks which allows for the exchange</p>
--	---

<p>20 U.S.C. 6777(e) 47 U.S.C. 254(h)</p> <p>18 U.S.C. 1460</p> <p>18 PA C.S. 5903</p>	<p>of information. It is the all encompassing term for a variety of computer services, including the World Wide Web, Gopher, Telnet, E-mail, FTP, IRC, NNTP, and all other TCP/IP-related services.</p> <p>Internet Relay Chat (IRC) – a form of instant communication over the Internet. It is mainly designed for group (many-to-many) communication in discussion forums called channels, but also allows one-to-one communication.</p> <p>LAN (local area network) – a group of computers and associated devices that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area (for example, within a building).</p> <p>Listserv – a small program that automatically redistributes e-mail to names on a mailing list. Users can subscribe to a mailing list by sending an e-mail note to a mailing list they learn about; listserv will automatically add the name and distribute future e-mail postings to every subscriber. (Requests to subscribe and unsubscribe are sent to a special address so that all subscribers do not see these requests.) These programs are also known as list servers.</p> <p>Malware – Malware (for "malicious software") is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware.</p> <p>Minor – in reference to the Children’s Internet Protection Act (“CIPA”), a minor is an individual who has not yet attained the age of seventeen. For other purposes, minor shall mean the age of minority as defined in the relevant law.</p> <p>Network – a series of devices interconnected by a communication pathway.</p> <p>Newsgroups (NNTP) – a newsgroup is a discussion about a particular subject consisting of notes written to a central Internet site and redistributed through Usenet, a worldwide network of news discussion groups. Usenet uses the Network News Transfer Protocol (NNTP).</p> <p>Obscene – under Federal law, analysis of the material meets the following elements: (a) whether the average person, applying contemporary community standards, would find that the material, taken as a whole., appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state or federal law to be obscene; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.</p> <p>Obscene – under Pennsylvania law, analysis of any material or performance meets the following elements:</p>
--	--

	<p>(a) the average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;</p> <p>(b) the subject matter depicts or describes in a patently offensive way, sexual conduct of a type described in this section; and</p> <p>(c) the subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.</p> <p>Passive user – those individuals who view the output or witness or encourage the actions or activities of an active user. Passive users are equally accountable for this usage Policy and are further required to report all inappropriate IT resource use to a teacher or administrator.</p> <p>Peer-to-Peer – on the Internet, peer-to-peer (referred to as P2P) is a type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and establish electronic communication.</p> <p>Phreaking – the use of information technology resources to make free telephone calls or to charge calls to another account.</p> <p>Piracy – the unauthorized and illegal reproduction of a copyrighted work or trademarked product.</p> <p>Plagiarism – taking the ideas or writings of others and presenting them as if they were original to the user.</p> <p>Remote access – the ability to get access to an IT resource from a location other than where the IT resource is located. This may include using dial-up or broadband Internet services, wireless communications or through a virtual private network (VPN).</p> <p>Right of publicity – a person’s right to protect his/her identity from unauthorized use. Identity may include a person’s name, nickname, picture, photograph, or any object closely identified with a person.</p> <p>RSS – RSS (RDF Site Summary - formerly called Rich Site Summary or Really Simple Syndication) is a method of describing news or other Web content that is available for "feeding" (distribution or syndication) from an online publisher to Web users.</p> <p>Security software – a collection of software products that insures the integrity of an IT resource. Examples include: anti-virus, anti-spam, firewall, machine policies, system scanners and monitors.</p> <p>Sexual Act/Contact – as defined at 18 U.S.C. § 2246(2) and 18 U.S.C. § 2246(3)</p>
--	--

	<p>Sexual Conduct – as defined at 18 PA C.S. §5903</p> <p>SMS – (Short Message Service) – is a service for sending messages to IT resources. SMS is similar to paging, which is the process of sending alert signals and/or data messages to a receiving device.</p> <p>Software - a general term for the various kinds of programs, applications or instructions used to operate computers, telecommunications, information technology resources, and/or electronic communications systems.</p> <p>Spam – Spam is a generic term encompassing all unsolicited electronic communications. It is typically referred to by users as “junk e-mail” but spam occurs in instant messages, on cell phones, via FAX or any other communications medium.</p> <p>Spidering – the practice of making temporary copies of Internet content to extract information for republication.</p> <p>Spoofing – a technique used to gain unauthorized access to a computer by sending electronic communications and pretending that these messages originate from a trusted source.</p> <p>Spyware – spyware is any technology that aids in gathering information about a person or organization without their knowledge.</p> <p>Staff – any person employed by the District or contracted into employment with the District.</p> <p>Student – any person enrolled in a District educational program.</p> <p>Telnet – a protocol which allows access to remote computers.</p> <p>Trojan horse – a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and perform its intended task.</p> <p>Unauthorized access – an attempt to use an IT resource without obtaining proper permission.</p> <p>Virtual Private Network (VPN) – a network that uses a public telecommunications infrastructure, such as the Internet, to provide remote users with secure access to their organization’s IT resources.</p> <p>Virus – in computers, a virus is a program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document. Viruses can be transmitted in an electronic communication or in a</p>
--	--

<p>18 U.S.C. 2256(5)</p> <p>4. Delegation of Responsibility</p>	<p>downloaded file, or be present on a storage medium. The immediate source of the electronic communication, downloaded file, or diskette you've received is usually unaware that it contains a virus. Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances cause their code to be executed by the computer. Some viruses are benign or playful in intent and effect and some can be quite harmful, erasing data or causing your hard disk to require reformatting.</p> <p>Visual Depiction - includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.</p> <p>WAN (wide area network) – a geographically dispersed telecommunications network.</p> <p>Warez – pirated commercial software that has been placed on an information technology resource for unauthorized distribution, access or use.</p> <p>Work use – use of IT resources for conducting necessary job description-related or specifically assigned tasks in furtherance of the operation of the District.</p> <p>World Wide Web – all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP) or related protocols for sharing information. Access to HTTP information typically requires a browser, though not always.</p> <p>Worm – a virus that replicates itself by resending itself as an e-mail attachment or as part of an electronic communication.</p> <p>Legitimate use of an IT resource does not extend to whatever an individual is capable of doing with it. Although some rules are built into the IT resources, these restrictions cannot limit completely what an individual can do or see. In any event, each user is responsible for his or her actions, whether or not rules are built-in and whether or not they can be circumvented.</p> <p>Users must be capable and able to use the District’s IT resources relevant to their responsibilities and must practice proper etiquette. They must also abide by the requirements of this and all District policies.</p> <p>Users are responsible for the security of their access account information. IT resource accounts will be used only by authorized owners of the accounts for authorized purposes.</p> <p>The District shall make every effort to ensure that IT resources are used for educational purposes and are used in a responsible manner by users. Due to the nature of the Internet as a global network, inappropriate materials, including those</p>
---	---

<p>5. Guidelines</p>	<p>which may be defamatory, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), inaccurate, obscene, sexually explicit, lewd, vulgar, rude, harassing, violent, inflammatory, threatening, terroristic, hateful, bullying, profane, pornographic, offensive or illegal may be accessed through IT resources and electronic communications systems. Because of the technology and design behind the Internet's operation, the District cannot completely block access to these resources. Any user who receives threatening or unwelcome communications shall immediately bring them to the attention of a teacher or administrator.</p> <p>The Director of Technology shall oversee IT resources and shall work with other administrators, faculty, staff, community leaders, regional or state organizations, or others deemed appropriate to ensure proper use of said resources, to educate users, provide leadership for proper training for all users in the use of IT resources and the requirements of this Policy, establish a system to ensure adequate supervision of the IT resources and interpret and enforce this Policy.</p> <p>The Director of Technology and/or designee shall establish a process for setting up IT resource access accounts, set quotas for IT resource usage, establish the District disaster prevention and recovery plan, and all other activities as deemed necessary for the successful operation of IT resources.</p> <p>Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information resources, to identify information appropriate to their age and developmental levels, and to evaluate and use IT resources to meet their educational goals.</p> <p>Students, staff and other users have the responsibility to respect and protect the rights of every other user in the District and connected to IT resources. Therefore, it is every user's responsibility to protect and safeguard IT resources with appropriate use of security software and to report detection of any unusual activity to a teacher or administrator.</p> <p>The building principals and/or designee, in conjunction with the Director of Technology, shall be responsible for determining what is inappropriate use based on applicable law, regulations and Board Policy. The building principals and/or designee shall be responsible for establishing a system to ensure adequate supervision of students using IT resources.</p> <p>The Director of Elementary Education and the Director of Secondary Education, in conjunction with the Director of Technology, shall ensure staff receive proper training in the use of IT resources and the requirements of this Policy.</p> <p>Users are expected to act in a responsible, ethical and legal manner and in</p>
----------------------	--

	<p>accordance with Board Policy, administrative regulations, guidelines, accepted rules of network etiquette and local, state, federal, and international law. All users shall execute an appropriate release prepared by the District which states the user has read and understands this Policy and its related rules, regulations and guidelines. Failure to execute this release may result in exclusion from IT resource use. The District reserves the right to determine if any activity not appearing in this Policy constitutes an acceptable or unacceptable use of the IT resources.</p> <p>These rules, regulations and guidelines are in effect any time District IT resources are accessed, whether on District property, when using mobile computing equipment, telecommunications facilities (in unprotected areas or environments, directly from home, or indirectly through another Internet service provider), and if applicable, when a user is accessing through their own equipment.</p> <p><u>All Users</u></p> <p><i>Personal Safety –</i></p> <p>Users shall promptly disclose to a teacher or administrator any electronic communication they receive that is inappropriate or makes them feel uncomfortable.</p> <p><i>Illegal/Unlawful Activities –</i></p> <p>Users shall not attempt to gain unauthorized access to any District or outside IT resources through use of District electronic communications systems or IT resources or go beyond their authorized access. This includes attempting to use IT resources as another user or access another person’s files.</p> <p>Users shall not attempt to and/or obtain personal information under false pretenses with the intent to defraud another person.</p> <p>Users shall not disrupt IT resource performance or alter, modify or destroy data.</p> <p>Users shall not use IT resources to engage in any illegal activity governed by local, state, federal and/or international law.</p> <p>IT resources shall not be used to advocate illegal drug use, whether expressed or through an implied pro-drug message. This does not include a restriction of political or social commentary on issues, such as the war on drugs or medicinal use.</p> <p>Users shall not plagiarize works they access through IT resources and shall respect the rights of copyright owners.</p> <p>Users shall not copy computer programs, software or other technology provided by the District for personal use. Users are not permitted to modify system setting of IT</p>
--	---

resources. The user shall not install, use, store, reproduce, distribute or transmit unauthorized and/or copyrighted or trademarked materials using IT resources.

System Security/Integrity –

The user shall be ultimately responsible for the use of his/her individual account and IT resources and all activity that occurs there. The user shall take all reasonable precautions to prevent other users from gaining access to and using the account. Users shall not share any account names and passwords with other users or leave IT resources logged in and unattended. The exception to this is when a Technology Department employee and/or designee requires the information in the course of their work duties.

At the end of a session, users shall properly log off an IT resource.

Users shall immediately notify a teacher or administrator if they have identified a possible security problem. Users however, shall not go looking for security problems, as this may be construed as an illegal attempt to gain access.

Users may not move, repair, configure, modify and/or attach external devices to IT resources. The exception to this rule is storage devices, such as USB drives. These storage devices must only be for data storage purposes and may not have any other configurations and/or capabilities (for example, MP3 (or other audio/video) players). External storage devices may not be used for bypassing security features or the IT resource boot or start-up process. In addition, applications, programs, games or other executable software may not be run from external storage devices. Vandalism or damage to IT resources shall require restitution for all costs associated with repair and/or replacement.

Users may not install computer hardware, peripheral devices, network or system hardware. The authority to install or connect hardware or devices on District IT resources or electronic communications systems is restricted to the Director of Technology and/or designee. All configurations and installations shall be made in accordance with the instruction manual provided with the device.

Access to all data on, taken from, or compiled using District IT resources is subject to inspection and discipline. Users have no right to expect that District information placed on users' personal IT resources and/or electronic communications systems is beyond the access of the District. The District reserves the right to legally access users' personal IT resources and/or electronic communications systems brought onto the District's property and/or to District events and/or connected to the District's IT resources and/or electronic communications systems, when the District reasonably believes they contain District information or contain information that violates Board Policy or contain data that the District reasonably believes involves criminal activity.

	<p>Users are prohibited from installing unauthorized devices, including attempts to create unauthorized network connections or any unauthorized extension or re-transmission of any IT resource or electronic communications system or service, whether wired, wireless, or by other means.</p> <p>Unauthorized scanning of District IT resources or electronic communications systems for security vulnerabilities is prohibited. Capture of data traversing IT resources or electronic communications systems (sometimes known as sniffing) is not permitted.</p> <p>Any user identified as a security risk or having a history of problems with other IT resources may be denied access to District IT resources.</p> <p>Food, drink, dangerous or caustic chemicals and/or any other substance which may cause damage to an IT resource are not permitted near the IT resource.</p> <p>IT resources shall be kept clear of clutter and shall be easily accessible by IT staff.</p> <p><i>Inappropriateness –</i></p> <p>Users shall not use IT resources to access inappropriate material. The District has taken precautions to restrict user access to inappropriate material. However, on a global network like the Internet and when users bring in personal IT resources, it is impossible to control all materials that a user may accidentally or purposefully discover. It is the user’s responsibility to avoid initiating access to inappropriate material. The District firmly believes that the valuable information and interaction gained by exposure to IT resources far outweighs the possibility that users may be exposed to materials not in keeping with his or her family’s values and beliefs. In addition, it is not possible for the District to monitor and enforce a wide range of social values when users access IT resources.</p> <p>Users shall not send, receive, view, download, access or transmit inappropriate matter and material likely to be offensive or objectionable to recipients including, but not limited to, that which may be defamatory, inaccurate, obscene, sexually explicit, lewd, hateful, 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, vulgar, rude, inflammatory, threatening, profane, pornographic, offensive, terroristic, and/or illegal.</p> <p>Users shall not use electronic communications systems or IT resources to cyberbully or harass another individual or entity.</p> <p>Users shall not transmit information that, if acted upon, could cause damage or danger of disruption to District operations or threaten the health, safety or welfare of any person or persons.</p>
--	--

	<p>Users failing to comply with requests from appropriate teachers, staff, or District administrators to discontinue activities that violate this Policy and/or threaten the operation or integrity of IT resources or electronic communications systems shall be subject to disciplinary measures.</p> <p>Expressed, written permission of the Superintendent and/or designee is required for the use of the name “Marple Newtown School District” or District building names, clubs, organizations, curricular/cocurricular/extracurricular activities in any form on a blog, discussion board, cast, chat or Internet page or website not owned or related to the District. When such permission is granted, the posting must specify that any statements made do not represent the position of the District.</p> <p>IT resources may not be used for commercial purposes. Users may not offer, provide or purchase products using IT resources unless prior approval has been solicited and received. Users shall not use IT resources to solicit business, advertise, or engage in any other selling activities in support of nonschool related fundraising or private business enterprises.</p> <p>Users shall not access or utilize IT resources for gambling, pools, or any other betting or games of chance.</p> <p>IT resources may not be used for political lobbying. IT resources can be used to communicate with elected representatives and express opinion on political issues, provided it is explicitly stated that the communication does not represent the view of the District.</p> <p>IT resources shall not be used for activities which may jeopardize the District’s tax exempt status. Users may not offer District IT resources for resale to individuals or organizations or use the District name in any unauthorized manner that would reflect negatively on the District, its employees, or students.</p> <p>User electronic communications conducted with IT resources may not be encrypted or otherwise altered to avoid security review and detection without the prior authorization of the Director of Technology and/or designee. Users must use District approved encryption to protect the confidentiality of sensitive or critical information in the District’s approved manner.</p> <p>Users shall not bypass or attempt to bypass Internet filtering or other security safeguards by any method.</p> <p><i>Respecting Resource Limits –</i></p> <p>Users shall respect limits placed upon their use of IT resources including time restrictions, file download size restrictions, e-mail size restrictions, storage quotas,</p>
--	--

	<p>and network bandwidth.</p> <p>Users shall not engage in spamming or initiate activity which deprives a user of an IT resource.</p> <p>IT resources shall not be used for recreational purposes or activities related to personal hobbies.</p> <p>The District is bound by its contractual and license agreement respecting certain third-party resources. Users are expected to comply with all such agreements when using IT resources.</p> <p><i>Services –</i></p> <p>The District reserves the right to determine what services will be provided through IT resources and electronic communications systems. Certain District authorized services, such as but not limited to blogs, social networking sites, wikis, casting, information feeds, collaboration tools, and other applications commonly referred to as Web 2.0 or Next Generation may be permitted by the District. When provided or authorized, such use will only occur after District authorized training is provided to users. Users must comply with Board Policy, administrative regulations and guidelines during such use.</p> <p><u>Student Users</u></p> <p><i>Personal Safety –</i></p> <p>Users shall not use IT resources to transmit personal contact information about themselves or other people. Personal contact information includes, but is not limited to, addresses (home, work, school), telephone numbers (home, cell, VoIP, work), webpage addresses and instant messenger identification.</p> <p>Users shall not use IT resources to arrange a meeting with someone without prior parental approval and participation.</p> <p><i>Inappropriateness –</i></p> <p>Unless the student receives prior permission and supervision from the student’s teacher or other appropriate school personnel, the student shall not use District IT resources, access the Internet, use e-mail (the only e-mail permissible is a District issued account, if provided. Students may not access web-based personal e-mail accounts), download or upload files from the Internet or disk, or subscribe to and participate in any discussion groups, mailing lists, or other electronic communication mediums.</p>
--	---

	<p><u>Staff Users</u></p> <p><i>Illegal/Unlawful Activities –</i></p> <p>The use of electronic communication to transmit confidential student information or sensitive personnel information is prohibited, except in an electronic communication that is sent directly to a parent/guardian, the subject of the e-mail or a school official. When sending an electronic communication that contains confidential information, the employee should refer to the subject of the e-mail by first name only (no initials, last name or other potentially identifying information). The District may employ the use of disclaimers or other methods of warning about the content of an electronic communication, however disclaimers have limited or no legal context. Staff must be mindful of privacy issues and regulations when sending electronic communications.</p> <p>The District is not responsible for lost or misdirected electronic communications and the nature of electronic communications does not ensure confidentiality. The exception to this is electronic communication that stays within District IT resources (i.e. an e-mail sent from one District internal e-mail account to another District internal e-mail account). However, if staff forward that communication outside District IT resources, they must take the precautions noted above before forwarding.</p> <p><i>System Security/Integrity –</i></p> <p>Certain employees may have remote access to District IT resources. This remote access will be treated in the same manner as if the employee were physically on District property and using IT resources. The employee’s remote computer must meet minimum configuration requirements and shall include security software.</p> <p>Staff shall keep a log of what students utilize what IT resources and staff shall inspect IT resources after use by students. Staff shall identify any damage or vandalism caused and the student responsible. Damage is anything that results from misuse of IT resources and would not normally occur in the course of ordinary use of the equipment. Vandalism is the intentional defacement or destruction of IT resources.</p> <p><i>Inappropriateness –</i></p> <p>When using IT resources for class activities, staff shall select material that is appropriate in light of the age of the students and is clearly relevant to the course objectives. Staff shall preview the electronic material and web sites they require or recommend for student access to determine the appropriateness of the material contained on or accessed through the site. Staff shall provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Staff shall assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions</p>
--	--

	<p>about controversial issues while demonstrating tolerance and respect for those who hold divergent views. Staff shall provide an orientation on acceptable use practices, fair use and copyright requirements and supervise students when using IT resources. District rules and regulations on the selection of curricular materials, if available, shall govern the selection process.</p> <p>Staff have the right to establish procedures in their area of supervision regarding IT resource use. Such local procedures should explicitly refer to this Policy and then add additional administrative regulations. No local procedures shall allow conduct that is prohibited by law, regulation or Board Policy.</p> <p><i>Respecting Resource Limits –</i></p> <p>Recognized bargaining units may have the right to use District IT resources as per the contract/agreement, if applicable.</p> <p>When using IT resources, staff shall subscribe to and participate in only high quality discussion group mail lists, list servers, online chats, RSS feeds, SMS texting, casting services, blogging, instant messaging, peer-to-peer services, or other electronic communication mediums that are relevant to their education or professional career development, if such services are made available.</p> <p>The use of e-mail to mass mail noneducational or nonwork related information is expressly prohibited.</p> <p>Staff are reminded of the District’s purpose for providing IT resources and electronic communications systems. Incidental personal use, as defined in this Policy, is permissible.</p> <p><u>Unacceptable Use Guidelines</u></p> <p>The District shall cooperate fully with service providers, local, state, federal, and/or international officials in any investigation concerning or relating to any suspected illegal or unauthorized activities conducted through District IT resources.</p> <p>In the event that there is an allegation that a user has violated this Policy, the user shall be provided with notification of the alleged violation and his/her privileges may be suspended immediately. During the course of an investigation into the incident, the user shall be given an opportunity to present an explanation for a final determination regarding continued access to IT resources.</p> <p>Disciplinary actions shall be tailored to meet the specific concerns related to the violation and to assist the user in gaining the self discipline necessary to behave appropriately when using IT resources. Users must be aware that violations of this Policy or other policies or for unlawful use of IT resources may result in loss of IT</p>
--	--

	<p>resource access and a variety of other disciplinary actions, including but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, or written reprimands, suspensions (with or without pay for employees), dismissals, expulsions and/or legal proceedings on a case-by-case basis. Consequences shall be issued consistent with the severity and frequency of the violation and previous unacceptable use.</p> <p>Guest users violating this Policy shall have access privileges immediately revoked and shall be subject to legal action and prosecution to the fullest extent of the law.</p> <p>The user is responsible for any damages to IT resources resulting from negligent, deliberate or willful acts committed by the user. The user shall also be responsible for incidental or unintended damage resulting from negligent, willful or deliberate violations of this Policy caused by the user. Vandalism shall result in cancellation of access to District IT resources and is subject to further discipline and/or restitution.</p> <p>References:</p> <p>Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.</p> <p>Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777</p> <p>Internet Safety – 47 U.S.C. Sec. 254</p> <p>Board Policy – 218, 233, 317, 814</p>
--	--