# DELAWARE VALLEY SCHOOL DISTRICT

SECTION: OPERATIONS

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

ADOPTED: NOVEMBER 19, 2009

REVISED: October 8, 2009

## 815. ACCEPTABLE USE OF COMMUNICATIONS AND CIS SYSTEMS

1. Purpose

The Delaware Valley School District ("School District") provides employees, students, and guests ("users") with hardware, software, and access to the School District's Electronic Communication System and network, which includes Internet access, whether wired, wireless, virtual or by any other means. Guests include, but are not limited to, visitors, workshop attendees, volunteers, adult education staff, children, School Board members, independent contractors, and School District consultants.

Computers, network, Internet, Electronic Communications, information technology systems, databases, files, software, and media (collectively called "CIS" systems) provide vast, diverse and unique resources. The Board of School Directors will provide access to the School District's CIS systems for users if there is a specific School District-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 District.

For users, the School District's CIS systems must be used for education-related purposes and performance of School District job duties in compliance with this policy. For employees, *Incidental Personal Use* of School District Computers is permitted as defined in this policy but they should not have an expectation of privacy in anything they create, store, send, receive, or display on or over the School District's CIS systems, including their personal files or any of their use the School District's CIS system. Students may only use the CIS systems for educational purposes and should not have an expectation of privacy in anything they create, store, send, receive, or display on or over the School District's CIS systems, including their personal files or any of their use the School District's CIS system.

For personal computers and technology devices brought onto the School District's property, or at School District events, or connected to the School District's network, if the School District reasonably believes the computers and/ or personal technology devices contain School District information or contain information that violates a School District policy, the legal rights of the School District or an other person, involves significant harm to the School District or an other person, or contains information/data that the School District reasonably believes involves a criminal

| | |
|---|---|
| | activity the personal technology device may be legally accessed to insure compliance with this policy, other School District policies, and to comply with the law. Users may not use their personal technology devices/Computers to access the School District's intranet, Internet or any other CIS system unless approved by the Director of Technology and/or designee, and/or authorized as part of the School District's services for users.<br><br>The School District 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 District assets and in lessening the risks that can destroy these important and critical assets. Consequently, users are required to fully comply with this policy, and to immediately report any violations or suspicious activities to their building administrator. 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 relevant School District policies. |
| 2. Definitions | |
| 18 U.S.C. §2256(8) | **1. 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:<br><br>a. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.<br><br>b. 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<br><br>c. 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. §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.<br><br>**2. Computer** - includes any School District owned, leased or licensed or user-owned personal hardware, software, or other technology used on School District premises or at School District events, or connected to the School District network, containing School 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, the School District 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, iPhones, MP3 players, thumb drives, cell phones (with or without Internet access and/or electronic mail and/or recording devices and/or camera/video and other capabilities), telephones, mobile phones or wireless devices, two-way radios/telephones, beepers, paging devices, laser pointers and attachments, and any other such technology hereafter developed.<br><br>**3. 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, electronic mail services, voicemail services, tweeting, text messaging, instant messaging, social networking, GPS, PDAs, facsimile machines, cell phones (with or without Internet access and/or electronic mail and/or recording devices, and/or cameras/video and other capabilities).<br><br>**4. Educational Purpose** - includes use of the CIS systems for classroom activities, professional or career development, and to support the School District's curriculum, policy and mission statement. |
| 20 U.S.C. § 6801<br><br>47 U.S.C. § 254(h)(7)(G) | **5. Harmful to Minors** - Under Federal law, any picture, image, graphic image file or other visual depictions that:<br><br>a. Taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex, or excretion;<br><br>b. 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.<br><br>c. taken as a whole lacks serious literary, artistic, political, educational or scientific value as to minors. |

| | |
|---|---|
| 18 Pa. C.S.A. § 5903 (e)(6) | Under Pennsylvania law, any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:<br><br>a. predominantly appeals to the prurient, shameful, or morbid interest of minors; and,<br><br>b. is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and,<br><br>c. taken as a whole, lacks serious literary, artistic, political, educational or scientific value for minors.<br><br>**6. Incidental Personal Use** - *Incidental Personal Use* of School District 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 District policies, procedures and rules, as well as Internet service provider ("ISP") terms, local, state and federal laws and must not damage the School District's CIS systems. |
| 20 U.S.C. § 6777 (e)<br>47 U.S.C. § 254 (h)(7)(D) | **7. Minor** - for purposes of compliance with the federal 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. |
| 18 U.S.C. § 1460<br>47 U.S.C. § 254(h)(7)(E) | **8. Obscene** - Under Federal Law, analysis of the material meets the following elements:<br><br>a. whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest;<br><br>b. 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<br><br>c. whether the work taken as a whole lacks serious literary, artistic, political, educational, or scientific value. |
| 18 Pa. C.S.A. § 5903 | Under Pennsylvania law, analysis of the material meets the following elements:<br><br>a. the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest.<br><br>b. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene. |

| | |
|---|---|
| | c. The subject matter, taken as a whole lacks serious literary, artistic, political, educational or scientific value. |
| 18 U.S.C. § 2246<br>18 Pa. C.S.A. § 5903<br>47 U.S.C. § 254(h)(7)(H) | **9. Sexual Act and Sexual Contact** - As defined at 18 U.S.C. § 2246(2), at 18 U.S.C.§ 2246(3), and at 18 Pa. C.S.A. § 5903. |
| 20 U.S.C. § 6801<br>47 U.S.C. § 254;<br>47 U.S.C. § 254(h)(7)(I) | **10. 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. § 1460 (b),<br>18 Pa.C.S.A. § 2256 | **11. Visual Depictions** - Undeveloped film and videotape and data stored on a Computer disk or by electronic means which is capable of conversion into a visual image but does not include mere words. |
| 3. Authority<br><br>24 P.S. § 5-510 | 1. Access to the School District'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 District. The School District, further reserves the right to deny access to prevent further unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The School District 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.<br><br>2. System administrators have the right to access by interception, and the stored communication of user accounts for any reason in order to uphold this policy and to maintain the system. **USERS SHOULD NOT HAVE AN EXPECTATION OF PRIVACY IN ANYTHING THEY CREATE, STORE, SEND, RECEIVE, OR DISPLAY ON OR OVER THE SCHOOL DISTRICT'S CIS SYSTEMS. INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THE SCHOOL DISTRICT'S CIS SYSTEMS.** The School District 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. § 6777<br>47 U.S.C. § 254 | 3. The School 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 School District 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. *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. Measures designed to restrict adults' and 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 or guardian for a student, and upon the written request from an adult presented to the Director of Technology.

4. The School District has the right, but not the duty, to inspect, review, or retain electronic communications created, sent, displayed, received, or stored on or over its CIS system to monitor (electronic or otherwise), record, check, track, log, access, or otherwise inspect and/or report all aspects of its for all users and of any user's personal computers, network, Internet, electronic communication systems, databases, files, software, and media that they bring onto School District property, or to School District events, that were connected to the School District network, which contained School District programs or School District or student data (including images, files, and other information), all pursuant to the law, in order to ensure compliance with this policy and other School District policies, to protect the School District's resources, and to comply with the law.

5. The School District 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:

a. Highest - uses that directly support the education of the students.

b. Medium - uses that indirectly benefit the education of the students.

c. Lowest - uses that include reasonable and limited educationally-related employee interpersonal communications and employee limited Incidental Personal Use.

d. Forbidden - all activities in violation of this Policy and local, state or federal law.

6. The School District additionally reserves the right to:

a. Determine which CIS systems services will be provided through School

| | |
|---|---|
| | District resources.<br><br>b. Determine the types of files that may be stored on School District file servers and computers.<br><br>c. View and monitor network traffic, fileserver space, processor, and system utilization, and all applications provided through the network and communications systems, including e-mail and other electronic communications systems<br><br>d. Remove excess e-mail or files taking up an inordinate amount of fileserver disk space after a reasonable time.<br><br>e. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and any other applicable School District policies occur or state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, and destruction of School District resources and equipment. |
| 4. Responsibility | 1. Due to the nature of the Internet as a global network connecting thousands of computers around the world, inappropriate matter, including those 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, sexting, flagging, location detection, bullying, profane, pornographic, offensive, and illegal, can be accessed through the network and electronic communications systems. Because of the nature of the technology that allows the Internet to operate, the School District 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 District policies.<br><br>2. Users must be capable and able to use the School District's CIS systems and software relevant to the employee's responsibilities. In addition, users must practice proper etiquette, School District ethics, and agree to the requirements of this policy. |
| 5. Delegation of Responsibility | 1. The Director of Technology and/or designee will serve as the coordinator to oversee the School District'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 insure adequate supervision of the CIS systems, maintain executed user agreements, and interpret and enforce this policy. |

| | |
|---|---|
| | 2. The Director of Technology and/or designee will establish a process for setting-up individual and class accounts, set quotas for disk usage on the system, establish the Record Retention and Record Destruction Policies and Records Retention Schedule to include electronically stored information (See School District Policies #800 and 800.1, and establish the School District virus protection process.<br><br>3. Unless otherwise denied for cause, student access to the CIS systems resources shall 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 District and School District CIS systems, and to abide by the rules established by the School District, its ISP, local, state and federal laws. |
| 47 U.S.C. § 254 (h)(5)(B)(iii). Policy 249. | 4. The Director of Technology and/or designee has the responsibility to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. |
| 6. Guidelines | 1. <u>Access To The CIS Systems</u><br><br>a. The CIS systems accounts of users will be used only by authorized owners of the accounts for authorized purposes.<br><br>b. An account will be made available according to a procedure developed by appropriate School District authorities.<br><br>c. CIS System. This policy, as well as other relevant School District policies, will govern use of the School District's CIS systems for users.<br><br>d. Types of Services include, but are not limited to:<br><br>(1) <u>Internet</u> - School District employees and students and guests will have access to the Web through the School District's CIS systems as needed.<br><br>(2) <u>E-Mail</u> - 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 designee at the recommendation of the teacher who will also supervise the students' use of the e-mail service.<br><br>(3) <u>Guest Accounts</u> – Guests may receive an individual web account with the approval of the Director of Technology and/or designee if there is a specific School District-related purpose requiring such access. Use of the CIS systems by a |

guest must be specifically limited to the School District-related purpose and comply with this policy and all other School District policies, procedures and rules, as well as ISP terms, local, state and federal laws and may not damage the School District's CIS systems. A School District Acknowledgment Form must be signed in writing, or electronically assent to, by a guest, and if the guest is a minor a parent's written or electronic signature is required.

(4) Blogs. Employees may be permitted to have School District sponsored blogs, after they receive training, and the approval of the Director of Technology. All bloggers must follow the rules provided in this policy and other applicable policies, regulations and rules of the School District.

(5) Web 2.0 Second Generation Web-based Services. Certain School District authorized Second Generation Web-based services, such as blogging, social networking sites, wikis, podcasts, RSS feeds, social software, folksonomies and collaboration tools that emphasize online educational collaboration and sharing among users may be permitted by the School District, however, such use must be approved by the Superintendent, or designee, followed by training authorized by the School District. Users must comply with this policy as well as any other relevant policy, regulations, and rules during such use, such as Copyright Policy # 814, and the School District's Copyright Guidelines Handbook.

e. Access to all data on, taken from, or compiled using School District Computers is subject to inspection and discipline. Users' have no right to expect that School District information placed on users' personal Ccmputers, networks, Internet, and electronic communications systems is beyond the access of the School District. The School District reserves the right to legally access users' personal technology devices brought onto the School District's property, or to School District events, or connected to the School District's network, when the School District reasonably believes they contain School District information or contain information that violates a School District Policy, the legal rights of the School District or an other person, involves significant harm to the School District or an other person, or contain information/data that the School District reasonably believes involves a criminal activity.

2. Parental Notification and Responsibility

The School District will notify the parents/guardians about the School District'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 District to monitor and enforce the wide range of social values in student use of the Internet. Further, the School District recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children. The School District

will encourage parents to specify to their children what material is and is not acceptable for their children to access through the School District's CIS system.

3. School District Limitation of Liability

The School District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the School District's CIS systems will be error-free or without defect. The School 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. Nor is the School District responsible for the accuracy or quality of the information obtained through or stored on the CIS systems. The School District 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 District shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The School District will not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the School District's CIS systems. In no event will 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.

4. Prohibitions

The use of the School District'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 District 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 District resources are accessed whether on School District property, 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 or when they publish a blog.

Students are prohibited from visually possessing and using their personal computers, as defined in this policy, on School District premises and property (including but not limited to, buses and other vehicles, at School District events, or through connection to the School District CIS systems, unless expressed permission has been granted by the teacher (after approval by the Director of Technology), who will then assume the responsibility to supervise the student in its use, or, unless an IEP team determines otherwise, in which case, an employee will supervise the student in its use. Thus, users are prohibited from using cell phones with or without Internet access and/or recording, and/or camera/video, and other capabilities and configurations. Cameras, and the like may not be used to take images of others, transfer them, or place them

| | |
|---|---|
| | on web sites without the consent of the building principal. Students who are performing volunteer fire company, ambulance or rescue squad functions, or need such a computer due to their medical condition, or the medical condition of a member of the family, with notice and the approval of the school administrator may qualify for an exemption of this prohibition.<br><br>***a. General Prohibitions***<br><br>Users are <u>prohibited</u> from using School District CIS systems to:<br><br>(1) Communicate about non-work or non-school related communications unless for incidental personal use and the employees' use comports with this policy's definition of incidental personal use.<br><br>(2) Send, receive, view, download, access 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, images or photograph whether by electronic data transfer or otherwise (commonly referred to as sexting, e-mailing, texting, among others). Neither may users advocate the destruction of property.<br><br>(3) Send, receive, view, download, access or transmit *Inappropriate Matter* as defined in this Policy. |
| Policy 249 | (4) Cyberbullying another individual or entity.<br><br>(5) Access or transmit gambling pools for money, including but not limited to, basketball and football, or any other betting or games of chance.<br><br>(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.<br><br>(7) Send terroristic threats, hateful mail, harassing communications, discriminatory remarks, and offensive, profane, or inflammatory communications.<br><br>(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 Director of Technology. |

(9) Facilitate any illegal activity.

(10) Communicate through e-mail for non-educational purposes or activities, unless it is for incidental personal use as defined in this policy. The use of e-mail to mass mail non-educational or non-work 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 District policies); conduct unauthorized fundraising or advertising on behalf of the School District and non-School District organizations; resale of School District Computer resources to individuals or organizations; or use the School District's name in any unauthorized manner that would reflect negatively on the School District, its employees, or students. *Commercial purposes* is defined as offering or providing goods or services or purchasing goods or services for personal use. School District acquisition policies will be followed for School District purchase of goods or supplies through the School District system.

(12) Engage in political lobbying.

(13) Install, distribute, reproduce or use copyrighted software on School District computers, or copy School District software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright. See the Copyright Infringement section in this policy, the School District's Copyright Policy, #814, and the School District's Copyright Guidelines Notebook for additional information.

(14) Install computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on School District computers is restricted to the Director of Technology and/or designee.

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

(16) Access, interfere, possess, or distribute confidential or private information without permission of the School District'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 District information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the School District'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 "Delaware Valley School District" in any form in blogs, on School District Internet pages or websites not owned or related to the School District, or in forums/discussion boards to express or imply the position of the School District without the expressed, written permission of the Superintendent. When such permission is granted, the posting must state that the statement does not represent the position of the School District.

(23) Bypass or attempt to bypass Internet filtering software by any method including, but not limited to, the use of anonymizer/proxies or any websites 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 Director of Technology and/or designee if they have identified a possible security problem. Users must read, understand, provide a signed Acknowledgement Form(s), and comply with this policy that includes network, internet usage, electronic communications, telecommunications, non-disclosure, and physical and information security policies. The following activities related to access to the School District's CIS systems, and information are prohibited:

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

(2) Acquiring or attempting to acquire 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 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 District 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 District 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 District.

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

(9) Users must protect and secure all electronic resources and information data and records of the School District from theft and inadvertent disclosure to unauthorized individuals or entities when they are under the supervision and control of the School District and when they are not under supervision and control of the School District, for example, but not limited to, working at home, on vacation or elsewhere. If any user becomes aware of the release of School District information, data or records, the release must be reported to the Director of Technology immediately. See the School District's Data Breach Policy # 816 for further information.

***c. Operational Prohibitions***

The following operational activities and behaviors are prohibited:

(1) Interference with 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 and trapdoor 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 robots 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 District 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 re-transmission of any computer, electronic communications systems, or network services, virtual, cloud, whether wired, wireless, cable, 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 District's electronic information.

(9) Intentionally destroying the School District's Computer hardware or software.

(10) Intentionally disrupting the use of the CIS systems.

(11) Damaging the School District'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 appropriate teachers or School District administrators to discontinue activities that threaten the operation or integrity of the CIS systems.

5. <u>Content Guidelines</u>

Information electronically published on the School District's CIS systems shall be subject to the following guidelines:

a. 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.

b. 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.

c. Documents, web pages, electronic communications, or videoconferences may not contain objectionable materials or point directly or indirectly to objectionable materials.

d. Documents, web pages and electronic communications must conform to all School District policies and guidelines, including the School District's Copyright Policy, #814 and the School District's Copyright Guidelines Handbook.

e. Documents to be published on the Internet must be edited and approved according to School District procedures before publication.

6. Due Process

a. The School District 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 District's CIS systems.

b. If students or employees possess due process rights for discipline resulting from the violation of this policy, they will be provided such rights.

c. The School District may terminate the account privileges by providing notice to the user.

7. Search and Seizure

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

b. The School District has the right, but not the duty, to inspect, review, or retain electronic communications created, sent, displayed, received, or stored on or over its CIS system to monitor (electronic or otherwise), record, check, track, log,

| | |
|---|---|
| | access, or otherwise inspect and/or report all aspects of its for all users and of any user's personal computers, network, Internet, electronic communication systems, databases, files, software, and media that they bring onto School District property, or to School District events, that were connected to the School District network, which contained School District programs or School District or student data (including images, files, and other information), all pursuant to the law, in order to ensure compliance with this policy and other School District policies, to protect the School District's resources, and to comply with the law. Users should not have an expectation of privacy in anything they create, store, send, receive, or display on or over the School District's CIS systems. Including their personal files or any of their use of the School District's CIS systems.<br><br>c. Everything that users place in their personal files should be written as if a third party will review it.<br><br>8. <u>Copyright Infringement and Plagiarism</u> |
| 17 U.S.C. § 101 et seq.<br><br>Policy 814 | a. Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through School District resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Employees will instruct users to respect copyrights, request permission when appropriate, and comply with license agreements. Employees will respect and comply as well.<br><br>b. 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 District does not permit illegal acts pertaining to the copyright law. Therefore, any user violating the copyright law does so at their own risk and assumes all liability.<br><br>c. 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; 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 District's computers is expressly prohibited. This includes all forms of licensed software -- shrink-wrap, clickwrap, browsewrap, and electronic software, downloaded from the Internet.<br><br>d. School District guidelines on plagiarism will govern use of material accessed through the School District's CIS systems. Users will not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices. Users understand that use of the School District's CIS Systems may involve the School District's use of plagiarism analysis software being applied to their work. |

| | |
|---|---|
| | 9. Selection of Material<br><br>a. School District policies on the selection of materials will govern use of the School District's CIS systems.<br><br>b. 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 will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will 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.<br><br>10. School District Web Site<br><br>The School District will establish and maintain a Web Site and will develop and modify its web pages that will present information about the School District under the direction of the Director of Technology and/or designee. Publishers must comply with this policy, and other School District policies for example, the School District's Web Site Development Policy # 819.<br><br>11. Blogging<br><br>a. If an employee, student or guest creates a blog with their own resources, the employee, student or guest may not violate the privacy rights of employees and students, may not use School District personal and private information/data, images and copyrighted material in their blog, and may not disrupt the School District.<br><br>b. 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 District policies. |
| 47 U.S.C. § 254 | 12. Safety and Privacy<br><br>a. To the extent legally required, users of the School District'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 Director of Technology and/or designee.<br><br>b. Users will not post, disclose, use, and disseminate personal contact information about themselves or other people on the CIS systems. The user may not steal another's identity in any way, may not use spyware, robots, cookies, or use |

School District or personnel employee technology or resources in any way to invade one's privacy. Additionally, the user may not disclose, use or disseminate confidential and personal information about students or employees. Examples include, but not limited to, using a using a PDA, iPod, MP3, Internet access and/or recording and/or cell phone with or without camera/video and including but not limited to, persons, places, and documents relevant to the School District, saving, storing and sending the image with or without text or disclosing them by any means, including but not limited to, print and electronic matter; revealing 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 District unless legitimately authorized to do so.

c. Student users will agree not to meet with someone they have met online unless they have parental consent.

13. Consequences for Inappropriate, Unauthorized and Illegal Use

a. 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 District policies, such as, but not limited to, the student and professional employee discipline policies, Code of Student Conduct, copyright, property , curriculum, terroristic threat, and harassment policies.

b. The user is responsible for damages to the network, equipment, electronic communications systems, and software resulting from negligent, deliberate, and willful acts. The user 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 District equipment, and recovery and/or breach of the data contained on them.

c. Violations as described in this policy may be reported to the School District, appropriate legal authorities, whether the Internet Service Provider (ISP), local, state, or federal law enforcement and may constitute a crime under state and/or federal law, which may result in arrest, e-mail prosecution, and lifetime inclusion on sexual offender registries. The School District will cooperate to the extent legally required with authorities in all such investigations.

| | |
|---|---|
| | d. Vandalism will result in cancellation of access to the School District's CIS systems and resources and is subject to discipline.<br><br>e. Any and all costs incurred by the School District 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.<br><br><u>References</u>:<br><br>PA Consolidated Statutes Annotated – 18 Pa. C.S.A. § 5903, 6312<br>PA Child Internet Protection Act – 24 P.S. § 4601 et seq.<br>PA Bullying Act – 24 P.S. § 1303.1-A<br>Digital Millennium Copyright Act – 17 U.S.C. § 1201<br>State Board of Education Regulations – 22 PA Code § 403.1<br>U.S. Copyright Law – 17 U.S.C. § 101 et seq.<br>United States Code – 18 U.S.C. § 1460, 2246, 2256, 20 U.S.C. § 6801<br>Enhancing Education Through Technology Act of 2001 – 20 U.S.C. § 6777<br>Federal Children's Internet Protection Act – 47 U.S.C. § 254<br>Board Policies – 249, 510, 800, 800.1, 814, 816, 819 |