Lehighton Area School District
1000 Union Street
Lehighton, PA 18235

Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Communications and Information Systems
Number	815
Status	
Legal	2. 20 U.S.C. 6777 4. 47 U.S.C. 254 6. 24 P.S. 1317.1 7. Pol. 237 8. 24 P.S. 1303.1-A 9. Pol. 814 10. Pol. 830 11. Pol. 220 12. Pol. 218 13. Pol. 233 14. 18 U.S.C. 2256 15. 18 Pa. C.S.A. 6312 16. 18 Pa. C.S.A. 5903 17. 18 U.S.C. 2246 18. 20 U.S.C. 9134 17 U.S.C. 101 et seq 24 P.S. 4601 et seq 47 CFR 54.520 Pol. 103 Pol. 104 Pol. 218.2 Pol. 248 Pol. 249 Pol. 348
Adopted	January 26, 2009
Last Revised	February 22, 2016

Purpose

The Lehighton School District (district) provides employees, students, and Guests (users) with access to the district's electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means. Guests include, but are not limited to, visitors, workshop attendees, volunteers, independent contractors, adult education staff, students, and Board members.

Computers, network, Internet, electronic communications and information systems (collectively CIS systems) provide vast, diverse and unique resources. The Board will provide access to the district's CIS systems for users if there is a specific district-related purpose to access information and research; to collaborate; to facilitate learning and teaching; consistent with the curriculum adopted by the district and to foster the educational purpose and mission of the district.

For users, the district's CIS systems must be used for education-related purposes and performance of district job duties. *Incidental personal use* of school computers is permitted for employees as 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 district policies, procedures and rules contained in this policy, as well as Internet service provider (ISP) terms, local, state and federal laws and must not damage the district's CIS systems. Students may only use the CIS systems for educational purposes. At the same time, personal technology devices brought onto the district's 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 contains information/data that the district reasonably believes involves a criminal activity may be legally accessed to ensure compliance with this policy, other district policies, and to comply with the law. Users may connect their personal electronics to the district's public wireless network. Personal electronics may not connect to the district's public wireless network or the wired network unless approved by the district's Information Technology department.

The 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 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 the Director of Information Technology. Conduct otherwise will result in actions further described in Consequences For Inappropriate, Unauthorized And Illegal Use, found in the last section of this policy, and provided in relevant district policies.

Definitions

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 one (1) or more of the following occurs:[14]

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit

conduct.

3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

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.[15]

Computer - includes any district-owned, leased or licensed or user-owned personal hardware, software, or other technology used on district premises or at district events, or connected to the district network, containing district programs or 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 district's and users': desktop, notebook, PowerBooks, tablet PC or laptop computers, printers, facsimile machine, cables, modems, Interactive Whiteboards and other peripherals; specialized electronic equipment used for students' special educational purposes; Global Positioning System (GPS) equipment; personal digital assistants (PDAs); iPods, MP3 players; cell phones, with or without Internet access and/or recording and/or camera/video and other capabilities, telephones, mobile phones, or wireless devices, two-way radios/telephones; beepers; paging devices, laser pointers and attachments, and any other such technology developed.

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 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 of 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, voice mail services, GPS, PDAs, facsimile machines, cell phones with or without Internet access and/or electronic mail and/or recording devices, cameras/video, and other capabilities.

Network - only district-owned equipment is allowed on the district wired network. Personal devices must utilize the district's public wireless network and adhere to the district's acceptable use policy. Personal electronic equipment may only be on the district's private wireless network or wired network if approved by the district's Information Technology department.

Educational Purpose - includes use of the CIS systems for classroom activities, professional or career development, and to support the district's curriculum, policy and mission statement.

Harmful to Minors - under federal law, any picture, image, graphic image file or other visual depictions that:[2][4]

1. Taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex, or excretion.

2. Depicts, describes, or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual content, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals.

3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value as to minors.

Under Pennsylvania law, any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:[16]

1. Predominantly appeals to the prurient, shameful, or morbid interest of minors.

2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors.

3. Taken as a whole, lacks serious literary, artistic, political, educational or scientific value for minors.

Incidental Personal Use - *Incidental personal use* of school computers is permitted for employees as 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 district policies, procedures and rules contained in this policy, as well as Internet service provider (ISP) terms, local, state and federal laws and must not damage the district's CIS systems.

Minor - for purposes of compliance with the Children's Internet Protection Act (CIPA), an individual who has not yet attained the age of seventeen (17). For other purposes, minor shall mean the age of minority as defined in the relevant law.[2][4]

Obscene - under federal law, analysis of the material meets the following elements:

1. Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest.

2. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically designed by the applicable state or federal law to be obscene.

3. Whether the work taken as a whole lacks serious literary, artistic, political, educational, or scientific value.

Under Pennsylvania law, analysis of the material meets the following elements:[16]

1. The average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest.

2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene.

3. The subject matter, taken as a whole lacks serious literary, artistic, political, educational or scientific value.

Sexual Act and Sexual Contact - as defined by state and federal law.[16][17]

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.[4][18]

Visual Depictions - undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image but does not include mere words.

Authority

Access to the 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 district, which 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 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.

It is often necessary to access user accounts in order to perform routine maintenance and security tasks; system administrators have the right to access by interception, the stored communication of user accounts for any reason in order to uphold this policy and to maintain the system. Users have no privacy expectation in the contents of their personal files or any of their use of the district's CIS systems. The district reserves the right to monitor, track, log and access CIS systems use and to monitor and allocate fileserver space.

The district reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through general policy, software blocking or online server blocking. Specifically, the district operates and enforces technology protection measure(s) that block or filter online activities of minors 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, 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, 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/guardian for a student, and upon the written request from an adult.[2][4]

The district has the right, but not the duty, to monitor, track, log, access and/or report all aspects of its computer information, technology and related systems of all users and of any user's personal computers, network, Internet, electronic communication systems, and media that they bring onto district property, or to district events, that were connected to the district network, which contained district programs or 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 district policies, to protect the district's resources, and to comply with the law.

The 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:

1. Highest - uses that directly support the education of the students.
2. Medium - uses that indirectly benefit the education of the students.
3. Lowest - uses that include reasonable and limited educationally-related interpersonal communications, and limited personal use.
4. Forbidden - all activities in violation of this policy.

The district additionally reserves the right to:

1. Determine which CIS systems' services will be provided through district resources.
2. Determine the types of files that may be stored on district fileservers and computers.
3. 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.
4. Remove excess e-mail or files taking up an inordinate amount of fileserver disk space after a reasonable time.
5. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and any other applicable 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 district resources and equipment.

Delegation of Responsibility

Due to the nature of the Internet as a global network connecting thousands of computers around the world, inappropriate materials, 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; bullying; profane; pornographic; offensive; or 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 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 Consequences For Inappropriate, Unauthorized And Illegal Use, found in the last section of this policy and as provided in relevant district policies.

Users must be capable and able to use the district's CIS systems and software relevant to their responsibilities. In addition, users must practice proper etiquette, district ethics, and agree to the requirements of this policy.

The Technology Director and/or designee will serve as the coordinator to oversee the 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 ensure adequate supervision of the CIS systems, maintain executed user agreements, and interpret and enforce this policy.

Staff accounts will be set up once the staff member is in the Payroll system and changes of staff information will go through the Payroll system. Once a staff member is no longer an employee of the district, all accounts will be locked.

Student accounts will be established when the school notifies IT on the student's enrollment in the school. The school will provide the student's name, ID number, and grade level via the IT Help Desk system. Student data will be deleted at the end of the school year.

The Technology Director and/or designee will establish the district virus protection process.

Unless otherwise denied for cause, student access to the CIS systems resources shall be through supervision by the professional staff and designated support 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 district and district CIS systems, and to abide by the rules established by the district, its ISP, local, state and federal laws.

Guidelines

Access to the CIS Systems

CIS systems user accounts will be used only by authorized owners of the accounts for authorized purposes.

An account will be made available according to a procedure developed by appropriate district authorities.

The district's Acceptable Use of the Computers, Network, Internet, Electronic Communications and Information Systems policy, as well as other relevant district policies, will govern use of the district's CIS systems for users.

Types of services include, but are not limited to:

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

2. E-Mail - district employees may be assigned individual e-mail accounts for work related use as needed.

3. Guest Accounts - guests may receive an individual domain account with the approval of the Technology Director and/or designee if there is a specific district-related purpose requiring such access. Use of the CIS systems by a guest must be specifically limited to the district-related purpose and comply with this policy and all other district policies, procedures and rules, as well as Internet Service Provider (ISP) terms, local, state and federal laws and may not damage the district's CIS systems. An agreement between the district and a guest, and a parental signature will be required if the guest is a minor.

4. Blogs - employees may only be permitted to have district-sponsored blogs, after they receive training, and the approval of the district. Use of the name of Lehighton Area School District in any form in web blogs, on district Internet website not owned or related to the district, or in forums/discussion boards to express or imply the position

of the Lehighton Area School District must be granted through written permission of the Superintendent. When such permission is granted, the posting must state that the statement does not represent the position of the district. All bloggers must follow the rules provided in this policy and other applicable policies, regulations and rules of the district.

Web 2.0 Second Generation Web-based Services - certain district-authorized Second Generation Web-based services, such as 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 district at the discretion of the classroom instructor.

Access to all data on, taken from, or compiled using district computers is subject to inspection and discipline. Users have no right to expect that district information placed on users' personal computers, networks, Internet, and electronic communications systems is beyond the access of the district. The district reserves the right to legally access users' personal technology devices brought onto the district's property, or to district events, or connected to the district's network, when the district reasonably believes they contain district information or contain information that violates a district policy, or contain information/data that the district reasonably believes involves a criminal activity.

Parental Notification and Responsibility

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

School District Limitation of Liability

The district makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the district's CIS systems will be error-free or without defect. The district does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the district, nor is the district responsible for the accuracy or quality of the information obtained through or stored on the CIS systems. The district shall not be responsible for any damage users may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using the computers, network and electronic communications systems. The district shall not be responsible for material that is retrieved through the Internet or the consequences that may result from them. The district shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the district's CIS systems. In no event shall the district be liable to the user for any damages whether direct, indirect, special or consequential, arising out of the use of the CIS systems.

Prohibitions

The use of the 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 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 district resources are accessed whether on 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.

Students may use the public wireless network as permitted by building administration and/or faculty designee. Students may not put personal electronic equipment on the district's wired network.

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 their family, with notice and the approval of the school administrator may qualify for an exemption of this prohibition.[6][7]

The use of the District Network, Internet, or any school computers for illegal, inappropriate, unacceptable, or unethical purposes are prohibited. The activities listed below are strictly prohibited **by all users** of the district network and school computers. The Lehighton Area School District reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the network. These prohibitions are in effect any time school district resources are accessed in anyway, whether in school or at another location, and whether connected directly to the school district network or computers or indirectly through another Internet service provider.

- Allowing another person to use an assigned account or password.
- Use of the network to transmit material likely to be offensive or objectionable to recipients.
- Use of the network to participate in inappropriate and/or objectionable news groups.
- Use of the network to transmit hate mail, harassment, discriminatory remarks, and other antisocial communications on the network.
- Use of the network to order or purchase in the name of the school district or in the name of any individual any type of merchandise or service, unless expressly authorized to do so as part of the user's employment duties. All costs to the district or any individual incurred because of this type of violation will be the responsibility of the user.
- Use of the network to subscribe to any fee-based on-line/Internet service, unless expressly authorized to do so as part of the user's employment duties. All costs to the district or any individual incurred because of this type of violation or any other unauthorized charges or fees resulting from access to the network or the Internet will be the responsibility of the user.
- Use of the network or school computers which results in any copyright violation.
- The unauthorized installation, distribution, reproduction or use of software on district computers or servers. Software may only be installed on district servers by the

Technology Department. Software may only be installed on district computers when expressly authorized by the Technology Department.

- Use of the network to intentionally obtain or modify files, passwords, or data belonging to other users, or to misrepresent other users on the network.
- Use of school technology or the network for fraudulent copying, communications, or modification of materials in violation of local, state, or federal laws.
- Destruction, modification, abuse, or unauthorized access to district computer hardware, software, or files including: loading, downloading, or use of unauthorized games, programs, files or other electronic media.
- Destruction of district computer hardware or software.
- Use of the network to participate in unauthorized Internet Relay chats or web-based chat rooms (on-line real-time conversations).
- Use of the network to facilitate unauthorized access, including all forms of "hacking", or any other illegal or unlawful activity.
- Use of network for unauthorized disclosure, use, or dissemination of personal identification information or other personal or confidential information of others.
- Use of the network by an employee for texting/instant messaging unless expressly authorized as part of the user's employment duties.
- Use of network by any student for texting/instant messaging unless such use is either (1) expressly authorized by an administrator and directly monitored by an administrator or professional staff, or (2) provided for under a students Individualized Education Program or Rehabilitation Act Section 504 Plan and directly or indirectly monitored by professional staff. The term "indirect monitoring" includes intermittent direct monitoring coupled with periodic review of usage logs to insure appropriate usage.
- Use of the network for commercial or for-profit purposes.
- Use of equipment in any manner that would disrupt network use by others.
- Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system.
- Use of the network to access or process pornographic or similar material.
- Use of the network by a minor to access visual depictions that are obscene, child pornography, or harmful to minors.
- Use of the network by an adult to access visual depictions that are obscene, child pornography, or harmful to minors unless necessary as part of the user's employment duties and no minors have access to the room in which the visual depictions are viewed.

- Use of a computer that has been logged in under another user's name, except where expressly authorized by the Technology Department for young students without network accounts, or other use of the network account or password of another user.

General Prohibitions –

Users are prohibited from using district CIS systems to:

1. Communicate about nonwork or nonschool related communications, unless for incidental personal use as defined in this policy.

2. Send, receive, view, download, access or transmit material that is harmful to minors, indecent, obscene, pornographic, child pornographic and terroristic. Neither may users advocate the destruction of property.

3. 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.

4. Cyberbully another individual or entity.[8]

5. Access or transmit gambling, pools for money, including but not limited to, basketball and football, or any other betting or games of chance.

6. Participate in discussion or news groups that cover inappropriate and/or objectionable topics or materials, including those that conform to the definition of inappropriate matter in this policy.

7. Send terroristic threats, hateful mail, harassing communications, discriminatory remarks, and offensive or inflammatory communications.

8. Participate in unauthorized Internet Relay Chats, texting/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 Technology Director and/or designee.

9. Facilitate any illegal activity.

10. Communicate through e-mail for noneducational purposes or activities, unless for incidental personal use as defined in the policy. The use of e-mail to mass mail noneducational or nonwork related information is expressly prohibited; for example, the use of the everyone distribution list, building level distribution lists, or other e-mail distributions 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 district policies; conduct unauthorized fund raising or advertising on behalf of the district and nonschool district organizations; resale of district computer resources to individuals or organizations; or

use the district's name in any unauthorized manner that would reflect negatively on the district, its employees, or students.

Commercial purposes are defined as offering or providing goods or services or purchasing goods or services for personal use. District acquisition policies will be followed for district purchase of goods or supplies through the district system.

12. Engage in political lobbying.

13. Install, distribute, reproduce or use copyrighted software on district computers, or copy district software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright. See the section for Copyright Infringement in this policy and the district's Copyright policy for additional information.[9]

14. Install computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on district computers is restricted to the Technology Director or designee.

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

16. Access, interfere, possess, or distribute confidential or private information without permission of the district's administration. An example includes accessing other students' accounts to obtain their grades.

17. Violate the privacy or security of electronic information.

18. Send any district information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the 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 Lehighton School District in any form in web blogs, on district Internet pages or websites not owned or related to the district, or in forums/discussion boards to express or imply the position of the Lehighton 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 district.

23. Bypass or attempt to bypass Internet filtering software by any method including, but not limited to, the use of anonymizers/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.

Access and Security Prohibitions –

Users must immediately notify the Technology Director 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, nondisclosure and physical and information security policies. The following activities related to access to the 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 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 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 district.

8. Users must protect and secure all electronic resources and information data and records of the district from theft and inadvertent disclosure to unauthorized individuals or entities when they are under the supervision and control of the district and when they are not under the supervision and control of the district, for example, but not limited to, working at home, on vacation or elsewhere. If any user becomes aware of the release of district information, data or records, the release must be reported to the Technology Director immediately. See the district's Breach of Computerized Personal Information policy No. 830 for further information.[10]

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

2. Altering or attempting to alter files, system security software or the systems without authorization.

3. Unauthorized scanning of the CIS systems for security vulnerabilities.

4. Attempting to alter any 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, 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 or pirating music files.

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

9. Intentionally destroying the district's computer hardware or software.

10. Intentionally disrupting the use of the CIS systems.

11. Damaging the district's CIS systems, networking equipment through the users' negligence or deliberate act.

12. Failing to comply with requests from appropriate teachers or district administrators to discontinue activities that threaten the operation or integrity of the CIS systems.

Consequences of Abuse of Responsibilities and Privileges

Any user of the network, who violates the prohibitions listed of this policy, engages in any other act determined to be an unacceptable use of the network by school authorities, or violates any other district policy governing use of school resources or copyright law, will have his or her user privileges revoked and may face other disciplinary procedures, up to and including suspension and expulsion of students and termination of employees. In addition, illegal use of the network, intentional deletion or damage to files of data, destruction of

hardware, copyright violations, or any other activity involving the violation of local, state, or federal laws will be reported to the appropriate legal authorities for prosecution.

Content Guidelines

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

1. Published documents including but not limited to audio and video clips or conferences, may not include a student's date of birth, social security number, driver's license number, financial information, credit card number, health information, phone number (s), street address, or box number, name other than first name, or the names of other family members without parental consent.

2. Documents, web pages, electronic communications, or videoconferences may not include personally identifiable information that indicates the physical location of a student at a given time without parental consent.

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

4. Documents, web pages and electronic communications, must conform to all district policies and guidelines, including the district's Copyright policy.[9]

5. Documents to be published on the Internet must be edited and approved according to district procedures before publication.[11]

Due Process

The district will cooperate with the district's ISP rules, local, state, and federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through the district's CIS systems.

If students or employees possess due process rights for discipline resulting from the violation of this policy, they will be provided such rights.[12][13]

The district may terminate the account privileges by providing notice to the user.

Search and Seizure

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

The district reserves the right to monitor, track, log and access any electronic communications, including but not limited to, Internet access and e-mails at any time for any reason. Users should not have the expectation of privacy in their use of the district's CIS systems, and other district technology, even if they use the CIS system for personal reasons. Further, the district reserves the right, but not the obligation, to legally access any personal technology device of students and employees brought onto the district's property or at district events, or connected to the district network, containing district programs or district or student data (including images, files, and other information) to insure compliance with this policy and other district policies, to protect the district's resources, to obtain information/data that the district reasonably believes involves criminal activity.

Everything that users place in their personal files should be written as if a third party will review it.

Copyright Infringement and Plagiarism

Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the 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.[9]

Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing the law. The 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.[9]

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 district's computers is expressly prohibited. This includes all forms of licensed software such as shrink-wrap, clickwrap, browsewrap, and electronic software downloaded from the Internet.[9]

District guidelines on plagiarism will govern use of material accessed through the district's CIS systems. Users will not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices.

Selection of Material

District policies on the selection of materials will govern use of the district's CIS systems.

When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers will 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.

School District Web Site

The district will establish and maintain a web site and will develop and modify its web pages that will present information about the district under the direction of the Technology Director and/or designee. Publishers must comply with this policy and other district's policies.

Blogging

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

district personal and private information/data, images and copyrighted material in their blog, and may not disrupt the district.

Conduct otherwise will result in actions further described in this policy and provided in relevant district policies.

Safety and Privacy

To the extent legally required, users of the district's CIS systems will be protected from harassment or commercially unsolicited electronic communication. Any user who receives threatening or unwelcome communications must immediately send or take them to the Technology Director and/or designee.

Users will not post 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, cookies, or use district or personal 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 are not limited to, using a PDA, iPod, MP3; cell phone with camera/video and Internet access to take pictures of anything, including but not limited to, persons, places, and documents relevant to the 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, reports, and resumes or other information relevant to seeking employment at the district unless legitimately authorized to do so.

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

Monitoring

In an effort to maintain a safe computing environment, district staff shall monitor the online activities of students to the extent feasible. Such monitoring may include both direct examinations of computers by teacher and other employees as well as remote technological monitoring tools. District staff may also monitor the online activities of employees through direct and remote means.

Consequences for Inappropriate, Unauthorized fnd Illegal Use

General rules for behavior, ethics, and communications apply when using the CIS systems and information, in addition to the stipulations of this policy. Users of the district equipment and/or network 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, suspensions (with or without pay for employees), dismissals, expulsions, and/or legal proceedings on a case-by-case basis. This policy incorporates all other relevant district policies, such as, but not limited to, the student and professional employee discipline policies, copyright policy, property policy, curriculum policies, terroristic threat policy, and harassment policies.

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

Illegal use of the network, intentional deletion or damage to files of data, destruction of hardware, copyright violations, or any other activity involving the violation of local, state, or federal laws will be reported to the appropriate legal authorities for prosecution.

Vandalism will result in cancellation of access to the district's CIS systems and resources and is subject to discipline.

Online Behavior

The school district will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

815-Attach-1.doc (27 KB) 815-Attach-2.doc (28 KB) 815-Attach.doc (30 KB)

Last Modified by Kim Frischkorn on March 4, 2016