Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Communications and Information (CIS) Systems
Code	815
Status	Active
Adopted	January 26, 2021

Purpose

The Nazareth Area School District ("school district") provides employees, students, and registered guests ("users") with school district limited electronic resources, including computers, hardware, software, and access to the school district's electronic communication systems, networks, which include Internet access, whether wired, wireless, cellular, virtual, cloud or by any other means, and electronic information sources, as detailed below. *Guests* include, but are not limited to, visitors, workshop attendees, volunteers, adult education staff and students, board members, independent contractors, and school district consultants and vendors.

Computers, electronic communication devices, mobile devices, networks, Internet, electronic communication systems and services, electronic information and data systems and services, databases, files, software, apps, media, video, and voice services, collectively called "CIS Systems," provide vast, diverse and unique resources. The Board of School Directors will make available access to the school district's CIS Systems for users if there is a specific school district-related purpose; for example, to access information; to research; to facilitate learning and teaching; to support school district business, and/or to foster the educational purpose and mission of the school district.

For users, the school district's CIS Systems must be used in compliance with this policy, other school district policies, regulations, rules, and procedures; Internet Service Provider ("ISP"), website, and app terms (if they are lawful); and local, state, and federal laws and procedures ("School District Policies and Other Legal Requirements"). Incidental personal use of school district authorized CIS Systems is permitted for employees as defined in this policy. However, the employees, as well as all other users should have no expectation of privacy in anything they create, store, send, receive, or display on or over the school district's hardware, software, and CIS Systems, including their personal files, or any of their use, for example, when users use their computer or electronic communication device or another entity's computer or electronic communication device(s) on the school district's CIS Systems at a school district location, event, or connect to the school district's network. Students may only use the CIS systems for educational purposes.

CIS Systems may include school district computers or electronic communication devices that are located or installed on school district property, at school district events, connected to the school district's networks or systems, or when using its mobile computing equipment, telecommunication facilities in protected and unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when users bring and use their own personal computers or personal electronic communications devices, or if relevant, when users bring and use another entity's computer or electronic communication devices to a school district location, event, or connect it to the school district network or systems.

If users bring personal computers or personal electronic communication devices onto school district property, to school district events, or connect them to the school district's network and systems, and if the school district reasonably believes that the personal computers and/or personal electronic communication devices contain school district information or contain information that violates school district policies and/or other legal requirements, the legal rights of the school district or another person,

or involve significant harm to the school district or another person, or involves a criminal activity, the personal computers or personal electronic devices may be legally accessed in accordance with the law to insure compliance with school district policies and/or other legal requirements. Users may not use their personal computers and personal electronic communication devices to access the school district's intranet, Internet or any other CIS System unless approved by the building principal and/or Assistant to the Superintendent for Educational Programs or designee.

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 the building principal and/or the Assistant to the Superintendent for Educational Programs or designee. Conduct otherwise will result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section found in the last section of this policy, and provided in other relevant school district policies, regulations, rules, and procedures.

This policy can be modified as the electronic information environment evolves.

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:[1]

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Under Pennsylvania law, any person who intentionally views or knowingly possesses or controls any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act is guilty of a felony of the third degree for their first offense, or guilty of a felony of the second degree for a second offense.[2]

Computer - Includes any school district owned, leased or licensed or user-owned hardware, software, or other technology used on school district premises or at school district events, or connected to the school district network and systems, containing school district programs or school district or student information and/or data (including images, and/or text, files) attached or connected to, installed in, or otherwise used in connection with a computer. For example, as applicable, computer includes, but is not limited to, the school district and users:[1][5]

1. Desktop, notebook, powerbook, tablet, chromebooks, netbooks, or laptop computers;
2. Servers, firewalls/security systems, distance learning equipment, video conference units, printers, facsimile machine, cables, modems, and other peripherals;
3. Specialized electronic equipment used for students' special educational purposes;
4. RFID, and Global Positioning System (GPS) equipment;
5. Personal digital assistants ("PDAs"), iPods, MP3 players, USB/jump drives;
6. iPads, Kindles, Nooks, and other electronic readers;

7. iPhones, cell phones (with or without Internet access and/or electronic mail and/or recording devices and/or camera/video and other capabilities and configurations), telephones, mobile phones or wireless devices, two-way radios/telephones and other smartphones;

8. Beepers, paging devices, laser pointers and attachments, Pulse Pens;

9. Wearable technology devices that can be worn by a person, either as an accessory or as part of material used in the clothing, and is able to be connected to the Internet enabling data to be exchanged between a network and the device (for example, smart watches, smart clothing, fitness trackers, and smart jewelry);

10. Computerized drones, and

11. 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, photo optical or photoelectronic facilities for the transmission/transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

Examples include, without limitation, the internet, intranet, voice mail services, electronic mail services, tweeting, text messaging, instant messaging, and social networking).

Educational Purpose - Includes use of the CIS Systems for classroom activities, professional or career development, and to support the school district's curriculum, policies, regulations, rules, and procedures, and mission statement.

Harmful to Minors - Under federal law, any picture, image, graphic image file or other visual depictions that:[3][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, and

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

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

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

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

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

Inappropriate Matter - Includes, but is not limited to visual, graphic, video, text and any other form of obscene, pornographic, sexually explicit, indecent, child pornographic, or other material that is harmful to minors. Examples include: taking, disseminating, transferring, or sharing, whether by electronic transfer (such as sexting, emailing, texting, among others) or otherwise hateful, illegal,

defamatory, lewd, vulgar, profane, inflammatory, threatening, harassing, discriminating (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/cyberbullying, flagging, terroristic, and other inappropriate matter and material specified throughout this policy, and other school district policies, regulations, rules, and procedures. It also includes advocating the destruction of property.

Incidental Personal Use - Incidental Personal Use of school district computers and CIS Systems 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, or is excessive. Personal use must comply with school district policies, and other legal requirements and must not damage the school district's CIS Systems.

Minor - For purposes of compliance with the federal Children's Internet Protection Act ("Fed 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.

Obscene - Under federal law, analysis of the material meets the following elements:[6]

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

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

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

Under Pennsylvania law, any material or performance, if:

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; and

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

Personal Electronic Communication Devices - Include laptops, chromebooks, mobile devices (for example, cell phones, smartphones, tablet devices (such as iPads and ereaders), wearable technology, drones, PDAs, pagers/beepers, location tracking devices, and cameras), electronic gaming systems, Google glasses, and any other devices that can capture still images or video, and can record, store, display transmit, or receive audio or video with digital, electronic, wired, wireless, or cellular communication capabilities that are not issued to a student by the school district.

Sexual Act and Sexual Contact - As defined at 18 U.S.C. § 2246(2), and at 18 U.S.C.§ 2246(3), 18 Pa. C.S.A. § 5903.[6][7]

Technology Protection Measure(s) - A specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornographic or harmful to minors.

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, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format, but does not include mere words.

Authority

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 unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The school district will cooperate with other educational entities, ISPs, websites, other appropriate authorities, and local, state and federal officials to the extent legally required in any investigation and following process and/or procedure concerning or related to the misuse of the CIS Systems, whether criminal or civil actions.[4][8][9]

It is often necessary to access users' accounts in order to perform routine maintenance and security tasks. System administrators have the right to access by interception, and to access the stored communication of users' accounts for any reason in order to uphold school district policies and other legal responsibilities, and to maintain the system. Users should have no privacy expectations in the contents or transmission of their personal files or any of their use of the school district's CIS Systems.

Users should have no 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. Users of the school district's CIS systems who transmit or receive communications and information shall be deemed to have consented to having the content of any such communication recorded, checked, received, monitored, tracked, logged, accessed and otherwise inspected or used by the school district, and to the monitoring and allocating fileserver space. Passwords and message delete functions do not restrict the school district's ability or right to access such communications or information.[4][10]

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, where possible, on its computers used and accessible to adults and students so as to filter or block inappropriate matter on the Internet as defined in this policy. Measures designed to restrict adults' and minors' access to material harmful to minors may be disabled to enable an adult or a student (who has provided written consent from a parent/guardian) to access bona fide research, not within the prohibitions of this policy, or for another lawful purpose. No person may have access to material that is illegal under federal or state law.[3][10]

Expedited review and resolution of a claim that this policy is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee, upon the receipt of written consent from a parent/guardian for a student, and upon the written request from an adult presented to the Assistant to the Superintendent for Educational Programs or designee.[8]

The school district has the right, but not the duty, to inspect, review, or retain electronic communication created, sent, displayed, received or stored on and over the school district's CIS Systems and to monitor (electronic or otherwise), record, check, track, log, access or otherwise inspect its CIS Systems.

In addition, in accordance with the law, the school district has the right, but not the duty, to inspect, review, or retain electronic communications created sent, displayed, received, or stored on user's personal computers, electronic communication devices, networks, Internet, electronic communications systems, and in databases, files, apps, software, and media that contain school district programs, information and/or data.

Also, in accordance with the law, the school district has the right, but not the duty, to inspect, review, or retain electronic communication created, sent, displayed, received or stored on another entity's computer or electronic communication device when users bring and use another entity's computer or electronic device to a school district location, event, or connect it to the school district network and/or systems, and/or that contains school district programs, or school district data or information.

The above applies no matter where the use occurs whether brought onto school district property, to school district events, or connected to the school district network, or when using mobile commuting equipment and telecommunications facilities in protected or unprotected areas or environments, directly

from home, or indirectly through social media or ISPs, as well as by other means. All actions must be conducted in accordance with the law, assist in the protection of the school district's resources, and insure compliance with school district policies and other legal Requirements.

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:

1. Highest - uses that directly support the education of the students, and business operations of the school district.

2. Medium - uses that indirectly benefit the education of the student, and business operations of the school district.

3. Lowest - uses that include reasonable and limited educationally-related employee interpersonal communications and employee limited incidental personal use.

4. Forbidden - all activities in violation of school district policies and/or other legal requirements.

The school district additionally reserves the right to:

1. Determine which CIS Systems' services will be provided through school district resources.

2. Determine the types of files that may be stored on school district file servers and computers.

3. View and monitor network traffic, fileserver space, processor, and system utilization, and all applications provided through the network and electronic communications systems and computers.

4. Remove excess email and other electronic communications or files taking up an inordinate amount of fileserver space after a reasonable time.

5. Revoke user privileges, remove user accounts, or refer to legal authorities, and/or school district authorities when violation of this and any other applicable school district policies and other legal requirements are violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, social media, vendor access, data breach, and destruction of school district resources and equipment.

Responsibility

Due to the nature of the Internet, inappropriate matter, as defined in this policy, can be accessed through the network and 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 district 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, regulations, rules, and procedures.

The school district must publish a current version of this policy so that all users are informed of their responsibilities. A copy of this policy, and the CIS Acknowledgement and Consent Form(s) must be provided to all users, who must sign the school district's CIS Acknowledgement and Consent Form(s), either by electronic or written means.

Employees must be capable and able to use the school district's CIS Systems and software relevant to the employee's responsibilities.

Delegation of Responsibility

The Assistant to the Superintendent for Educational Programs 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, and other school district policies, regulations, rules, and procedures, establish a system to insure adequate supervision of the CIS Systems, maintain executed User CIS Acknowledgement and Consent Forms, and interpret and enforce school district policies, and/or other legal requirements.

The Assistant to the Superintendent for Educational Programs or designee will establish a process for setting-up individual and class accounts, set quotas for usage, establish a Record Retention and Records Destruction Policy and a Records Retention and Destruction Schedule to include electronically stored information, and establish the school district virus protection process.[11]

Unless otherwise denied for cause, student access to the CIS Systems resources must be through supervision by the professional staff. Administrators, teachers and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of the resources. All users have the responsibility to respect the rights of all other users within the school district and others using the school district CIS Systems, and to abide by the school district's policies, and/or other legal requirements.

The building principal 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.[4][13][17]

If necessary, the Superintendent is granted the authority to create, modify, update, and enforce an administrative regulations to accompany this policy.

Guidelines

Access to the CIS Systems

The CIS Systems' accounts of users must be used only by authorized owners or designees of the accounts and only for authorized purposes.

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

CIS Systems – School district policies, and other legal requirements will govern use of the school district's CIS Systems for users.

Types of services include, but are not limited to:

1. Internet - School district employees, students, and guests will have access to the Internet through the school district's CIS systems, as needed.

2. Email, text messaging, and video conferencing - School district employees may be assigned individual email, text message, and Skype accounts for work-related use, as needed. Students may be assigned individual email accounts, as necessary, by the Assistant to the Superintendent for Educational Programs or designee at the recommendation of the teacher who will also supervise the students' use of the email service. Students and guests may not be assigned text message and Skype accounts.

3. Guest accounts – Registered guests may receive an individual Internet account with the approval of the Assistant to the Superintendent for Educational Programs 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 school district policies, and/or other legal requirements, and may not damage the school district's CIS Systems. A school district CIS Acknowledgment and Consent Form must be signed, in writing or electronically, by a guest, and if the guest is a minor, a parent's/guardian's written or electronic signature is required.

4. Blogs - Employees may be permitted to have school district-sponsored blogs, after they receive training, and the approval of the Assistant to the Superintendent for Educational Programs or

designee. All bloggers must follow the rules provided in this policy and all other school district applicable policies (for example, the school district's Social Media Policy), regulations (for example, the school district's Social Media Administrative Regulations), and other legal requirements.

5. Web 2.0 Second Generation and Web 3.0 Third Generation Web-based Services - Certain school district authorized Second Generation and Third Generation Web-based services, such as blogging, authorized social networking sites, wikis, podcasts, RSS feeds, social software, folksonomies, course management systems, and collaboration tools that emphasize online participatory learning (where users share ideas, comment on one another's project, plan, design, or implement, advance or discuss practices, goals, and ideas together, co-create, collaborate and share) among users may be permitted by the school district; however, such use must be approved by the building principal and/or Assistant to the Superintendent for Educational Programs or designee and/or Technology Advisory Committee, followed by training authorized by the school district. Users must comply with this policy, other relevant school district policies and other legal requirements during such use.

Parental Notification and Responsibility

The School District will notify the parents/guardians about the School District's CIS Systems and the School District's Policies, regulations, rules, and procedures 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 a 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/guardians to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the School District's CIS Systems. Parents/Guardians are responsible to help monitor their child(ren)'s use of the school district's CIS Systems when they are accessing the network and systems.[8]

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 computers, networks and electronic communications systems. The school district will 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.[8]

Student Use of Electronic Communication Devices

The possession and Silent Use of Electronic Communication Devices, including Personal Electronic Communication Devices, by School District students when in compliance with the Electronic Communication Devices Policy, other School District Policies, and Other Legal Requirements, and supportive of the educational program of the School District, is permitted. However, the possession and use of Electronic Communication Devices, including Personal Electronic Communication Devices, by students that are found to be disruptive to the educational process and/or environment can be abusive in ways that negatively affect students, employees, and the School District's mission and environment, and is prohibited in accordance with this Policy, other School District Policies, and Other Legal Requirements.

Safety

It is the district's goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, email, social networking websites, etc.[4][27]

Internet safety measures shall effectively address the following:

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.
2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.
5. Restriction of minors' access to materials harmful to them.

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, at school district events, while connected to the school district's network, when using mobile commuting equipment, telecommunication facilities in protected and unprotected areas or environments, directly from home, or indirectly through another ISP, website, or app, and if relevant, when an employee or student uses their own equipment, or another entity's equipment.[5]

General Prohibitions -

Users are prohibited from using school district CIS Systems to:

1. Communicate about non-work or non-school related matters, unless the employees' use comports with the definition of incidental personal use in this policy.
2. Send, receive, view, upload, download, store, access, print, post, distribute or transmit material that is harmful to minors, indecent, obscene, pornographic, child pornographic, terroristic, sexually explicit, or sexually suggestive. This includes but is not limited to visual depictions. Examples include, taking, disseminating, transferring or sharing obscene, pornographic, lewd or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (such as, sexting, emailing, texting, among others). Users must not advocate the destruction of property.[12]
3. Send, receive, view, upload, download, store, access, print, distribute, or transmit Inappropriate Matter as defined in this policy, and material likely to be legally offensive or objectionable to recipients.
4. Cyberbully another individual or entity. See school district's Bullying/Cyberbullying Policy 249.[13]
5. Access or transmit gambling information or promote or participate in 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.[12][14][15][16]

8. Use in an illegal manner or to facilitate any illegal activity.

9. Communicate through email or text messages for non-educational purposes or activities, unless it is for incidental personal use as defined in this policy. The use of email to mass mail non-educational or non-work related information is expressly prohibited (for example, the use of the "everyone" distribution list, or all staff lists, building-level distribution lists or other email distribution lists to offer personal items for sale is prohibited).[4][13][17]

10. 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; engage in the 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 must be followed for school district purchase of goods or supplies through the school district system.

11. Engage in political lobbying.

12. Install, distribute, reproduce or use unauthorized 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 Handbook for additional information.[18]

13. 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 Assistant to the Superintendent for Educational Programs or designee.

14. 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.

15. 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.

16. Violate the privacy or security of electronic information.

17. 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.

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

19. Post personal or professional web pages on the school district's website without administrative approval.

20. Post anonymous messages.

21. Use the name of the "Nazareth Area 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, and social media sites, to express or imply the position of the Nazareth Area School District without the expressed, written permission of the Superintendent or designee. When such

permission is granted, the posting must state that the statement does not represent the position of the school district.

22. Bypass or attempt to bypass Internet filtering software by any method including, but not limited to, the use of anonymizers/proxies, tunnels, SSH terminals, or any websites that mask the content the user is accessing or attempting to access.

23. 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.

24. Attempt to and/or obtain personal information under false pretenses with the intent to defraud another person.

25. Use location devices to invade a person's privacy or to harm or to put another person in jeopardy.

26. Plagiarize works that are found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as they were yours.

27. Post false statements, or steal the identity of another person.

Access and Security Prohibitions -

Users must immediately notify the Assistant to the Superintendent for Educational Programs or designee if they have identified a possible security problem. Users must read, understand, and submit a signed CIS Acknowledgement and Consent Form(s), and comply with this policy that includes network, Internet usage, electronic communications, telecommunications, nondisclosure, and physical and information security requirements. The following activities related to access to the school 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 user IDs and passwords of another. Users are required to use unique strong passwords that comply with the school district's password, authentication, and syntax requirements. Users must not acquire or attempt to acquire the user ID, passwords, security questions and authentication information of another. Users will be held responsible for the result of any misuse of users' names, passwords, security questions, and authentication information 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 acts would include, but not be limited to, 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 website that the school district has filtered or blocked as unauthorized. Examples include, but are not limited to, unauthorized social media, music and video download and gaming

sites.

9. Installing or attaching keylogging devices, keylogging mechanisms or keylogging software of any kind.

10. Using an app with students that is not approved by the school district's authorized committee and/or designated administrator.

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 at all times. If any user becomes aware of the release of school district information, data or records, the release must be reported to the Director of Curriculum, Instruction and Technology or designee immediately.

Operational Prohibitions -

The following operational activities and behaviors are prohibited:

1. Interference with, infiltration into, or disruption of the CIS Systems, network accounts, services or equipment of others, including, but not limited to: the propagation of computer "worms" and "viruses", Trojan Horse, trapdoor, robot, spider, crawler or program code; the sending of electronic chain mail or distasteful jokes; and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts. Users may not hack or crack the network or others' computers, whether by malware or spyware designed to steal information, or viruses and worms or other hardware or software designed to damage the CIS systems, or the systems of others, 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.[11][19]

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, whether wired, wireless, cable, virtual, cloud, cellular or by other means.

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

7. Loading, downloading, or using unauthorized apps, games, programs, files, or other electronic media, including, but not limited to, downloading unauthorized music and video 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 computers, 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.

Content Guidelines

Information electronically published on the school 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 user'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 the consent of the user, and if relevant, parent/guardian.

2. Documents, web pages, electronic communications, or video conferences 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 video conferences may not contain objectionable materials or point directly or indirectly to objectionable materials.

4. Documents, web pages and electronic communications, must conform to school district policies, and other legal requirements.

5. Documents to be published on the Internet must be edited and approved according to school district policies, regulations, rules, and procedures before publication.

Due Process

The school district will cooperate with the school district's ISP's 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. If students or employees possess due process rights for discipline resulting from the violation of the school district's policies, and other legal requirements, they will be provided such rights.[20][21][22]

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

Search and Seizure

Users' violations of school district policies, and other legal requirements 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.

The school district reserves the right, but not the duty, to inspect, review, or retain electronic communications created, sent, displayed, received, or stored on or over its CIS Systems; to monitor, record, check, track, log, access or otherwise inspect; and/or report all aspects of its CIS Systems. This includes items related to any personal computers, network, Internet, electronic communication systems, databases, files, software, and media that individuals may bring onto school district's property, or to school district's events, that were connected to the school district's network, and/or that contain school district programs, or school district or users' data or information, in accordance with the law, in order to insure compliance with school district policies, and other legal requirements to protect the school district's resources, and to comply with the law.

Users should have no 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.

Everything that users place in their personal files should be entered with the knowledge and understanding that it is subject to review by a third party.

Copyright Infringement and Plagiarism

Federal laws, cases, policies, regulations, and guidelines pertaining to copyright will govern the use of material accessed through the school district's resources. See school district Copyright Policy 814. Users must make a standard practice of requesting permission from the holder of the work, or complying with the Fair Use Doctrine, and/or complying with license agreements. Employees will instruct users to respect copyrights, request permission when appropriate, and to comply with the Fair Use Doctrine, and/or license agreements. Employees will respect and comply as well.[18]

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.

Violations of copyright law include, but are not limited to, making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over computer networks, remixing or preparing mash-ups that violate the law, and deep-linking and framing into the content of others' websites. 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 whether acquired by shrink-wrap, clickwrap, browsewrap, or electronic software and apps downloaded from the Internet.[18][23]

No one may circumvent a technology protection measure(s) that controls access to a protected work unless they are permitted to do so by law. No one may manufacture, import, offer to the public, or otherwise traffic in any technology, product, service, device, component or part that is produced or marketed to circumvent a technology protection measure to control access to a copyright protected work.

School district guidance on plagiarism will govern use of material accessed through the school district's CIS Systems. Users must not plagiarize works. 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 works.

Selection of Material

Relevant school district policies, regulations, rules, and procedures on the selection of materials will govern use of the school 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 must preview the materials, apps, and websites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the website. Teachers must provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers must assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.[24]

School District Website

The school district has established and maintains a website and will develop and modify its web pages that will present information about the school district under the direction of the building principal or designee. Publishers must comply with school district policies, and other legal requirements.

The school district may limit its liability by complying with the Digital Millennium Copyright Act's safe harbor notice and takedown provisions.

Blogging

If a user creates a blog with their own resources and on their own time, the user may not violate the privacy rights of employees and students, may not use school district personal and private information/data, images, equipment, resources and infringed copyrighted material in their blog, and

may not disrupt the school district. See also the school district's Social Media Policy, and its accompanying administrative regulations.

Contrary conduct 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, and other legal requirements.

Safety and Privacy

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 provide or show them to the Assistant to the Superintendent for Educational Programs or designee.[25]

Users must not post unauthorized personal contact information about themselves or other people on the CIS Systems. Users may not steal another's identity in any way, may not use spyware, cookies, or other program code, keyloggers, and may not use school district or personal technology or resources in any way to invade another's privacy. Additionally, users may not disclose, use or disseminate confidential and personal information about students or employees, unless legitimately authorized to do so. Examples include, but are not limited to, revealing biometric data, student grades, Social Security numbers, dates of birth, home addresses, telephone numbers, school addresses, work addresses, credit card numbers, health and financial information, evaluations, psychological reports, educational records, reports, and resumes or other information relevant to seeking employment at the school district.

If the school district requires that data and information be encrypted, users must use school district authorized encryption to protect their security.

Students, by their use of the school district's CIS System, agree not to meet with someone they have met online unless they have parent(s)/guardian(s) consent.

Cloud, Virtual, and Online Storage of School District Information and Data

Users must keep all school district information (including but not limited to employees and students) in the school district's and its contracted parties' storage, unless permission is granted in writing by the Superintendent or designee. This means that employees, students, and guests must not place school district information in cloud, virtual or online storage beyond the control, access, protection and safety of the school district unless specific permission is granted in writing by the Superintendent or designee and the student, employee and guest agree to the school district's terms and conditions, including but not limited to safety, security, privacy, location and school district access.[4][19]

Consequences For Inappropriate, Unauthorized and 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, other school district policies, and/or other legal requirements. Users must be aware that violations of this policy or other school district policies, and/or other legal requirements, or for unlawful use of the CIS Systems, may result in loss of CIS Systems' 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), dismissal, expulsions, breach of contract, and/or legal proceedings. This will be handled 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, social media, data breach, property, curriculum, terroristic threat, vendor access, student electronic communication devices, and harassment policies.

The user is responsible for damages to computers, the network, equipment, electronic communications systems, and software resulting from accidental, negligent, deliberate, and willful acts. Users will also be responsible for incidental or unintended damage resulting from negligent, willful, or deliberate violations of school district policies, and/or other legal requirements. 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 information and/or data contained on them.

Violations as described in this policy, other school district policies, and other legal requirements may be reported to the school district, and to appropriate legal authorities, whether ISPs, websites, or apps, and local, state, or federal law enforcement. Actions that constitute a crime under state and/or federal law could result in arrest, criminal prosecution, and/or lifetime inclusion on sexual offenders registries. The school district will cooperate to the extent legally required with authorities in all such investigations.

Vandalism will result in cancellation of access to the school district's CIS Systems and resources and, the user is subject to discipline.

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 school district policies, and/or other legal requirements, shall be paid by the user who caused the loss.

Legal

1. 18 U.S.C. 2256
2. 18 Pa. C.S.A. 6312
3. 20 U.S.C. 7131
4. 47 U.S.C. 254
5. Pol. 237
6. 18 Pa. C.S.A. 5903
7. 18 U.S.C. 2246
8. 24 P.S. 4604
9. 24 P.S. 510
10. 24 P.S. 4610
11. Pol. 800
12. Pol. 218.2
13. Pol. 249
14. Pol. 103
15. Pol. 103.1
16. Pol. 104
17. 24 P.S. 1303.1-A
18. Pol. 814
19. Pol. 830
20. Pol. 218
21. Pol. 233
22. Pol. 317
23. 17 U.S.C. 101 et seq
24. 17 U.S.C. 1202
25. 17 U.S.C. 512
26. Pol. 840
27. 47 CFR 54.520

18 Pa. C.S.A. 2709

24 P.S. 4601 et seq

Pol. 220