Greater Nanticoke Area School District

Policy No. 815

SECTION: Operations

TITLE: ACCEPTABLE USE OF COMPUTER NETWORK AND THE INTERNET

ADOPTED: June 21, 2012

REVISED: May 1, 2023

815. ACCEPTABLE USE OF COMPUTER NETWORK AND THE INTERNET

1. Purpose

The Greater Nanticoke Area School District recognizes that information technology tools and network. facilities are used to support learning and to enhance instruction. Information technology tools and network facilities allow people to interact with many other computers and networks. It is a general policy that all technologies are to be used in a responsible, efficient, ethical, and legal manner.

The use of the Greater Nanticoke Area School District's information technology tools and network facilities shall be consistent with the district's mission and the curriculum adopted by the Greater Nanticoke Area School District.

2. Definitions

CIPA - The Children's Internet Protection Act (CIPA) is a federal law enacted to address concerns about access to offensive content over the Internet on school and library computers. CIPA requirements include the following three items:

1. Technology Protection Measure - A technology protection measure is a specific technology that blocks or filters Internet access. It must protect against access by adults and minors to visual depictions that are obscene, child pornography, or - with respect to use of computers with Internet access by minors - harmful to minors. It may be disabled for adults engaged in bona fide research or other lawful purposes. For schools, the policy must also include monitoring the online activities of minors.
2. Internet Safety Policy - The Internet safety policy must address, access by minors to inappropriate matter on the Internet The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications, unauthorized access including

"hacking" and other unlawful activities by minors online, unauthorized disclosure, use, and dissemination of personal information regarding minors, and measures designed to restrict minors' access to harmful materials.

3. Public Notice and Hearing -The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing to address a proposed technology protection measure and Internet safety policy.

CHILD - The term child means an individual under the age of 13 defined in Children's Online Privacy Protection Act of 1998.

Child pornography - means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

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

Definition from Section 2256 of Title 18, United States Code.

COPPA - Children's Online Privacy Protection Act applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age. It details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing to those under 13.

Educational purpose - includes use of the information technology tools, network facilities, and Internet access for classroom activities, professional or career development, and to support the school district's curriculum, policy, and mission statement.

Hacking - any attempt to gain unauthorized access (or the unauthorized access) to network facilities or using district network facilities to attempt or to gain unauthorized access to other networks or computing resources.

Harmful to minors - any picture, image, graphic image file or other visual, sound, or written depiction

that:

1. Taken as a whole, and with respect to minors, appeals to an inappropriate 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 contact, actual or simulated, normal or perverted sexual acts or a lewd exhibition of the genitals.
3. Lacks serious literary, artistic, political, or scientific value as to minors; depicts extreme violence; promotes intolerance.

Definition from 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254

HIPPA - Health Insurance Portability and Accountability Act, pertaining to the Privacy Rule for Protected Health Information. The Protected Health Information is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

Illegal activities/uses - any use of network facilities which violates a municipal ordinance, or local, state, or federal law, including those activities relating to intellectual property rights, trade secrets, the distribution of obscene or pornographic materials or the Family Educational Rights and Privacy Act.

Information technology - any electronic device, computer hardware and software, operating systems, web-based information and applications, telephones and other telecommunications products, video equipment and multimedia products, information kiosks and office products such as photocopiers and fax machines.

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

Network facilities –

1. Computer hardware and software, electronic connections, electronic devices, and other information technology tools used for information processing, as well as peripheral devices connected to these tools.
2. Network bandwidth including Internet bandwidth and other devices necessary to facilitate network connectivity such as e-mail services, fileservers, routers, switches, hubs, firewalls, premise wiring, network data ports, etc.
3. Computers hardware and software, electronic connections, electronic devices and other information technology tools used on district property or used off district property that impacts the district or causes a disruption to the educational environment, or when such use comes in conflict with the Student Code of Conduct or district policy, whether or not such tools are owned by the district and whether or not they are connected physically or wirelessly to the district's information network(s).
4. Computers, electronic connections, electronic devices, and other information technology tools while they are connected remotely (from home or elsewhere) to the district's network.

Online collaboration - using site-based or web-based technology tools to communicate and work productively with other users to complete educationally relevant tasks.

Personal use - incidental personal use of school computers is permitted for employees so long as such use does not interfere with the employee's job duties and performance, with system operations or with other system users.

Personal use must comply with this policy and all other applicable district's procedures and rules contained in this policy, as well as ISP terms, local, state, and federal laws; and must not damage the district's information technology tools, network facilities and Internet access systems.

Staff - includes administrative, teaching, support and volunteer personnel employed by or voluntarily affiliated with the Greater Nanticoke Area School District.

Technology Protection Measure - a specific technology that blocks or filters Internet access.

Technology tools - 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 school 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. Technology equipment includes, but is not limited to, district and users': desktop, notebook, netbook, tablet PC or laptop computers, servers, firewalls/security systems, distance learning equipment, videoconference units, printers, facsimile machine, cables, modems, and other peripherals, specialized electronic equipment used for students' special educational purposes, Global Positioning System (GPS) equipment, personal digital assistants (PDAs), iPods, MP3 players, USB/jump drives, cell phones, with or without Internet access and/or recording and/or camera/video and other capabilities and configurations, telephones, mobile phones, or wireless devices, two-way radios/telephones, beepers, paging devices, laser pointers and attachments and any other such technology developed.

Telecommunications - any system that allows users access to a wide variety of information from electronic networks found on local, state, national and international databases, Internet or intranet servers and other information technology tools. Examples include, but are not limited to, Internet technologies, e-mail, Internet-based discussion groups and bulletin boards.

---

3. Authority

The Board of Directors (Board) establishes that use of information technology tools and network facilities impacting the district is a privilege, not a right.

Inappropriate, unauthorized, and illegal use may result in cancellation of the privileges of users and appropriate disciplinary action consistent with the district's disciplinary code.

The information available to students and staff does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received.

All network and computing resources must meet requirements for established policies, procedures and conditions of the Greater Nanticoke Area School District and any external entity administrating resources to which the network or computing resources are connected.

The district's Director of Technology, or other authorized school employees, may at any time review the subject, content and appropriateness of electronic communications, Internet access, usage of the district's information technology or other electronic files and remove them or block the inappropriate use as warranted, or report any violation of these rules to the district's administration or appropriate law enforcement officials. The district reserves the right to remove a user account from its network facilities to prevent further unauthorized or illegal activity if this activity is discovered.

The hardware, software, messages transmitted, and electronic files created on it are the property of the district.

Users have no expectation of privacy or confidentiality in the content of electronic communications, Internet access or other electronic files sent and received utilizing the district's information technology tools, network facilities or stored in his/her directory. The Greater Nanticoke Area School District reserves the right to monitor, inspect, copy, review, and store at any time, without prior notice, all usage of its information technology, network facilities and Internet usage and all information transmitted or received in connection with such usage. All such information files and user accounts shall be and remain property of the district.

---

4. Delegation of Responsibility

The district shall make every effort to ensure that district resources are used responsibly by students and staff. Students and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet.

All staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, to evaluate and use the information to meet their educational goals and practice proper etiquette and ethical use of district resources.

The district shall not be responsible for any information lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet. The district is not responsible for any unauthorized charges or fees resulting from access to the Internet.

The Board of Directors for the Greater Nanticoke Area School District endorses the use of technology as an integral part of the district's instructional program.

The Superintendent or designee shall be responsible for the development of educational programs using technology and global networks and shall establish procedures for the development of such programs.

The Superintendent or designee shall be responsible for developing procedures used to determine whether the district's technology tools and network facilities are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:

1. Utilizing a technology protection measure that blocks or filters Internet access for minors or adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board or their designee.
2. Maintaining and securing a usage log.
3. Monitoring online activities of all users.

Unless otherwise denied for cause, student access to onsite district resources shall be through supervision by the district staff. All users have the responsibility to respect the rights of all other users within the district and district's technology resources and to abide by the rules established by the district, its ISP, and local, state and federal laws.

---

5. Guidelines

Network accounts will be used only by the authorized owner of the account for its approved purpose. These accounts will be made available according to a procedure developed by appropriate district authorities. All communications and information accessible via the network should be assumed to be the property of the district and shall not be disclosed. Network users shall respect the privacy of other users on the system.

A guest may receive an individual network account with the approval of the Director of Technology and/or designee if there is a specific district-related purpose requiring such access after the AUP is signed and must comply with this policy and all other district policies, procedures, and rules, as well as local, state, and federal laws. An agreement between the district and a guest will be required. A parental signature will be required if the guest is a minor.

Prohibitions

The use of district information technology tools, network facilities and the Internet for illegal, inappropriate, or unethical purposes by students or staff is prohibited. More specifically, the following are prohibited:

1. Use of the network for commercial or for-profit purposes, product advertisement, political lobbying or to facilitate illegal activity.
2. Hacking, port scanning, unauthorized attempts to access network resources, creating malicious code, phishing, spamming or use of the network to develop programs that harass other users or infiltrate a computer system and/or damage the software components of a computer or system.

3. The illegal installation, distribution, reproduction, or use of copyrighted material on district information technology or network facilities.
4. Accessing or transmitting files dangerous to the integrity of the district's information technology or network facilities.
5. Attempting to circumvent or disable any filter, information security or other security measure.
6. Attempting to use network facilities while access privileges are suspended or revoked.
7. Use of the network to access materials, images or photographs that are obscene, pornographic, lewd, or otherwise illegal.
8. Use of the network to transmit material likely to be offensive, objectionable, or inflammatory to recipients such as hate mail, harassment, or discriminatory remarks.
9. Use of the network to misrepresent other users on the network, forge electronic mail messages or quote personal communications in a public forum without the original author's prior consent.
10. Loading or use of unauthorized games, programs, files, or other electronic media.
11. Use of district information technology tools or network facilities to disrupt the work of others; intentionally disrupt information network traffic or crash the network and connected systems; and the hardware or software of other users shall not be destroyed, modified, or abused in any way.
12. Use of the network which results in any copyright violation or other contracts violating such matters as institutional or third-party copyright, license agreements and other contracts.
13. Posting of anonymous messages, possessing any data which might be considered a violation of these rules in paper, electronic or any other form or using inappropriate language or profanity.
14. Revealing personal information or passwords related to any users on the network other than by district staff in the performance of assigned duties.
15. Use of any social networking or communication medium on campus that causes a disruption to the educational process (e.g., posting inflammatory comments about another student or staff member).
16. Attaching personal technology tools directly to the network without the express permission of the Director of Technology.

Security

To the greatest extent possible, users of the district's network will be protected from harassment and unwanted or unsolicited communication. The security of network facilities is protected through the use of passwords.

Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of network facilities and the safety of users, the following guidelines shall be followed:

1. Users shall not reveal their passwords to another individual or use any other user's password. If a user suspects someone else has his/her password, the password shall be changed immediately by district personnel.
2. Users are responsible to log off a computer or secure the computer when it is not in use and are not permitted to use a computer that has been logged in under another user's name.
3. Any user identified as a security risk or having a history of problems with other electronic resources may be denied access to the network.
4. The use of technology tools for the purpose of online collaboration and communication within and among users is a privilege, not a right. Furthermore, any collaborative tool user accounts created by district personnel or by the end-user for the purpose of completing course curriculum are subject to the guidelines defined by the Acceptable Use Policy of the Greater Nanticoke Area School District, regardless of where the access to that technology tool has taken place.
5. Any network user who receives threatening or unwelcome communications or an invitation from Internet contacts to an inappropriate face-to-face meeting shall immediately report the incident to a teacher or administrator.
6. Student users shall not reveal personal information to other users through the Internet, etc. that could identify themselves or other users or allow a person to locate a user.
7. Users shall not intentionally seek information on, obtain copies of or modify files, other data or passwords belonging to other users.
8. Users shall not transfer or download confidential data or data that contains sensitive personally identifiable information via any portable storage devices including USB devices.
9. Users should exercise due diligence in regard to printing confidential data or data that contains sensitive personally identifiable information, including grade reports, health records, IEP's and other records subject to the Health Insurance Portability and Accountability Act.

Filtering

Any district computer/server utilized by students and staff shall be equipped or connected to with Internet blocking/filtering software or hardware. The district will also monitor online activities of users through direct observation or technological means to ensure adherence to this policy. Internet filtering software or other technology-based protection systems may be disabled by the Director of Technology or his/her designee, as necessary, for purposes of valid research or other educational projects being conducted by users, as determined and approved by a building administrator.

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 when using electronic communications and other forms of direct electronic communications.
3. Prevention of unauthorized online access, including "hacking" and other unlawful activities.

4. Unauthorized disclosure, use, and dissemination of personal information.
5. Restriction of access deemed by the district to be harmful to minors.
6. Restriction of access to visual depictions that are obscene, child pornography or harmful to minors.

Disclaimer of Warranties/Indemnification

The district makes no warranties of any kind, either express or implied, in connection with this policy, access to and use of its information technology, or network facilities. The district shall not be responsible for any claims, losses, damages, or costs (including fees) of any kind suffered, directly or indirectly, by any user of his/her parents(s)/guardian(s) arising out of the use of its information technology or network facilities under this policy. Further, the district is not responsible for damage that may occur as a result of an individual user attempting to connect a personal technology device to any district-owned device.

By signing this policy, the user is taking full responsibility for his/her use, and the user who is eighteen (18) or older, or, in the case of a user under eighteen {18), the parents(s)/guardian(s) are agreeing to indemnify and hold the district administrators, professional employees and staff harmless from any and all losses, cost claims or damages resulting from the user's access to its network facilities, including, but not limited to, any fees or charges incurred through purchases of goods or services by the user. The user, or if the user is a minor, the user's parent(s)/guardian(s) agree to cooperate with the district in the event of the district's initiating an investigation of a user's access to the computer network and the Internet.

Actions Resulting from Misuse

Deliberate and/or negligent abuse of the network, computing resource or any other district resource could lead to disciplinary action. Any such action would be subject to applicable procedures established by the district. The network user, whether student or employee may be responsible for restitutions for damages to the equipment, systems or software resulting from negligent, deliberate, or willful acts.

All incidents of misuse are to be reported to building principals responsible for the students and staff. The building principal or his designee will conduct an investigation to determine the participant and the extent of the misuse.

Consequences of violations include but are not limited to:

1. Suspension of information network access; revocation of information network access; suspension of network privileges; revocation of network privileges; suspension of computer access; revocation of computer access.
2. Revocation of district issued technology tools, including all mobile devices owned by the district.
3. Employment suspension; school suspension.
4. Employment termination; school expulsion.
5. Legal action and prosecution by the authorities.

Copyright

The illegal use of copyrighted software by students and staff is prohibited.

All software installed on district technology must be approved by the Director of Technology for the purposes of network security and licensing.

Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.

Safety

To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report such immediately to a teacher or administrator. Students shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc.

Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software or connected to content filtering through the network.

Internet safety measures shall effectively address the following:

1. Control of access by minors to inappropriate matter on the Internet.
2. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.
3. Unauthorized disclosure, use and dissemination of personal information regarding minors.
4. Restriction of minors' access to materials harmful to them.

Any network user who receives threatening or unwelcome communication shall immediately bring them to the attention of a teacher or administrator. Network users shall not reveal personal addresses or telephone numbers to other users on the network.

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 cyber bullying awareness and response.

Remedies and Recourses

Anyone accused of any violation has all the rights that would normally apply if such person were accused of school vandalism or any other illegal activity.

The district has the right to restrict or terminate information network access at any time for any reason. The district further has the right to monitor network activity in any form that it sees fit to maintain the integrity of the information network.

Procedure for Handling Request to Reconsider Information/Materials

No duly selected materials whose appropriateness is challenged shall be removed from the school except upon the recommendation of a review committee, as provided for below, with the concurrence of the Superintendent.

The following procedures are to be observed:

1. All complaints to staff members shall be reported to the building principal, whether received by telephone, letter or in personal conversation.
2. The principal shall contact the complainant to discuss the complaint and attempt to resolve it informally by explaining the philosophy and goals of the school district and/or the library media center.
3. If the complaint is not resolved informally, the complainant shall be supplied with Greater Nanticoke Area School District's network policy statement, the procedure for handling objections and a complaint form. The complaint form must be completed and returned before consideration will be given to the complaint.
4. When the request is returned, the reasons for selection of the specific information shall be reestablished by the appropriate staff.
5. In accordance with statement of philosophy, no questioned materials shall be removed from the school pending a final decision. Pending the outcome of the request for consideration, however, access to questionable materials can be denied to the child (or children) of the parents/guardians making the complaint, if they so desire.
6. Upon receipt of a completed objection form, the principal in the building involved will call together a committee to consider the complaint. This committee may consist of the principal, the Director of Technology, a teacher, the department chair, a member of the community and a librarian.
7. The committee shall meet to discuss the material, following the guidelines set forth in the network policy, and shall prepare a report on the material containing their recommendations on disposition of the matter.
8. The principal shall notify the complainant of the decision and send a formal report and recommendation to the Superintendent. If the committee decides to keep the work that caused the complaint, the complainant shall be given an explanation. If the complaint is valid, the principal will acknowledge it and make recommended changes.
9. If the complainant is still not satisfied, s/he may appeal to the Superintendent who shall make a final determination of the issue. The Superintendent may seek assistance from outside organizations, such as the American Library Association, the Association for Supervision and Curriculum Development, etc., in making his/her determination.

References:

School Code - 24 P.S. Sec. 1303.1-A

Children Internet Protection Act - 47 U.S.C. Sec. 254

Enhancing Education Through Technology Act of 2001- 20 U.S.C. Sec.6777

Internet Safety- 47 U.S.C. Sec. 254

Code of Best Practices in Fair Use for Media Literacy Education - Temple University

ACCEPTABLE USE OF COMPUTER NETWORK AND THE INTERNET

DISTRICT INFORMATION TECHNOLOGY TOOLS, NETWORK FACILITIES AND INTERNET ACCESS

CONSENT AND WAIVER

The following form must be read and signed by you and your parent or legal guardian.

By signing this Consent and Waiver form, I _____ (print name) and my parent(s)/guardian(s) agree to abide by the following restrictions. I have discussed these rights and responsibilities with my parent(s)/guardian(s).

Further, my parent(s)/guardian(s) and I have been advised that the district does not have control of the information on district information technology tools and network facilities, although it attempts to provide prudent and available barriers. Other sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate, or potentially offensive to some people. While the Greater Nanticoke Area School District's intent is to make Internet access available to further its educational goals and objectives, account holders will have the ability to access other materials as well.

The district believes that the benefits to educators and students from access to district information technology tools and network facilities, in the form of information resources and opportunities for collaboration, far exceed any disadvantages of access. Ultimately, the parent(s)/guardian(s) of minors are responsible for setting and conveying the standards that their student should follow. To that end, the district supports and respects each family's right to decide whether or not to apply for Greater Nanticoke Area School District network access.

The student and his/her parent(s}/guardian(s) must understand that student access to the Greater Nanticoke Area School District network exists to support the district's educational responsibilities and mission. The specific conditions and services that are offered will change from time to time. In addition, the Greater Nanticoke Area School District makes no warranties with respect to the Greater Nanticoke Area School District network service, and it specifically assumes no responsibilities for:

1. The content of any advice or information received by a student from a source outside the district or any costs or charges incurred as a result of seeing or accepting such advice.
2. Any costs, liability or damages caused by the way the student chooses to use his/her district network access.
3. Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the district.
4. While the Greater Nanticoke Area School District supports the privacy of electronic mail, students must assume that this cannot be guaranteed.

By signing this form, I agree to the following terms:

1. My use of the Greater Nanticoke Area School District's network must be consistent with the Greater Nanticoke Area School District's goals.
2. I will not use the Greater Nanticoke Area School District network for illegal purposes of any kind.
3. I will not use the Greater Nanticoke Area School District network to transmit threatening, obscene, or harassing materials. The district will not be held responsible if I participate in such activities.
4. I will not use the Greater Nanticoke Area School District network to interfere with or disrupt network users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms and viruses, and using the network to make unauthorized entry to any other machine accessible via the network.
5. It is assumed that information and resources accessible via the Greater Nanticoke Area School District network are private to the individuals and organizations which own or hold rights to those resources and information unless specifically stated otherwise by the owners or holders of rights. Therefore, I will not use the Greater Nanticoke Area School District network to access information or resources unless permission to do so has been granted by the owners or holders of rights to those resources or information.

Student Name: _____ Grade: _____ (please print)

Student Signature: _____ Date: _____

Student's School: _____

Date of Birth: _____

Parent/Guardian:

As the parent/guardian of this student, I have read the Acceptable Use Policy. I understand that this access is designed for educational purposes. Greater Nanticoke Area School District has taken precautions to eliminate controversial materials. However, I also recognize it is impossible for Greater Nanticoke Area School District to restrict access to all controversial materials, and I will not hold them responsible for materials acquired on the network; therefore, I agree to accept responsibility for guiding my child and conveying to him/her appropriate standards for selecting, sharing and/or exploring information and media.

Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission for my child to use district information technology tools and network facilities and the Internet, and certify that the information contained on this form is correct.

Parent/Guardian Name: _____ (please print)

Signature: _____ Date: _____

Telephone: _____ Email Address: _____