NORTHERN BEDFORD COUNTY SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF INTERNET, COMPUTERS AND NETWORK RESOURCES

ADOPTED: December 2, 2004

REVISED: April 10, 2012

815. ACCEPTABLE USE OF INTERNET, COMPUTERS AND NETWORK RESOURCES

1. Purpose

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. The district has taken precautions to restrict access to controversial materials. However, on a global network it is impossible to control all materials and an industrious user may discover controversial information. The district firmly believes that the valuable information and interaction available on the worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the district.

The district provides students, staff and other authorized individuals with access to the district's computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means.

The Internet shall be used to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work. Use of the network must be in support of education and research and consistent with the educational objectives of the district.

2. Authority

The availability of access to electronic information does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.

Pol. 218, 233, 317, 417, 517	The Board declares that computer and network use is a privilege, not a right. The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the district's Internet, computers or network resources, including personal files or any use of the district's Internet, computers or network resources. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources. The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the appropriate supervisor or technology department.
3. Delegation of Responsibility	Administrators, teachers and 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, evaluate and use the information to meet their educational goals, and utilize technology resources in a lawful and responsible manner. The primary function of the district's network facilities is to provide opportunity for professional productivity of our employees and the academic growth of the students we serve. When using the district's information technology tools and network facilities, students and staff have the responsibility to respect and protect the rights of every other user in the district and those they communicate with or interact with on the Internet. The district directs that in compliance with the Child Internet Protection Act (CIPA) every teacher will review key points of the Technology and Acceptable Use Policy with their students at the start of the school year and will monitor, enforce, and immediately report any suspicious activity or violation to the appropriate supervisor or technology department. The district will make a diligent effort to supervise the use of the Internet by students to assure that they will not be accessing information other than what would be useful to the learning process. The district shall make every effort to ensure that this resource is used responsibly by students and staff. Students shall agree to use the Internet only as specifically directed or permitted by teachers or others acting in a similar capacity to teachers. The building administrator shall have the authority to determine what is inappropriate use.

	The appropriate supervisor or the technology department shall be responsible for implementing technology initiatives, procedures, and data collection to determine how technology is used and whether the district's information technology and network facilities are being used for purposes prohibited by law and this policy. These procedures shall include but not be limited to:
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 CFR Sec. 54.520	1. Utilizing a content filter which is updated and maintained by the district's technology department, cannot be turned off at the workstation level when students or adults are logged on to the computer for Internet use, and blocks and/or filters Internet access for minors and 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 filtering software vendor. With rapid growth and expansion of the Internet daily, all inappropriate URL's cannot be guaranteed. Upon notification of an inappropriate site to the network administrator, filtering can be started immediately. 2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
4. Guidelines	All district employees and students will be given a network account for school related use. Accounts are made available according to a procedure developed by school district authorities. Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed to be district property. Network users shall respect the privacy of other users on the system. Students should be aware that all administrators, teachers, and staff have access to student folders should the need arise to place documents into a folder, retrieve files from a student folder, or to review the actions of a student's use on the network. Types of services available on the network, but are not limited to the following: 1. **Internet** – District employees, students, and guests will have access to the Internet through the district's network. All district employees must have a signed Technology Acceptable Use Agreement on file in order to be granted permission to use the Internet on the NBCSD campus.

	A Technology and Acceptable Use Agreement form signed by students and parents/guardians must be on file for each student, Pre-K-12. Students not having the appropriate paperwork on file will be prohibited from Internet use. Students caught using the Internet without the appropriate paperwork on file will be subject to appropriate disciplinary action. Student work and likeness may be posted with either the first name only, or the first name and last initial, but at no time should a student's full name be displayed. Photographs of minors may only be posted with prior written consent of the parent/guardian with a signed media release form on file in the school office.
Pol. 815.1	**2.** **E-Mail** – District employees are assigned individual e-mail accounts for work-related use. Students in grades 6-12 are assigned individual e-mail accounts for school-related used through Google Apps for Education. All students in grades 6-7 must have a signed parent permission-form allowing the student to have e-mail. 3. **Guest Accounts** – Guests may receive an individual network account or access to the Internet only with the approval of the Director of Technology, and/or designee, if there is a specific school district-related purpose requiring such access. Use of the network and/or internet by a guest must be specifically limited to the school/district-related purpose and comply with this policy and all other school district policies, regulations, procedures, and rules, as well as local, state and federal laws and may not damage the school district's network systems. 4. **Blogs** – Employees may be permitted to have school district-sponsored blogs through the school website. All bloggers must follow the rules provided in this policy, and other applicable policies, regulations, rules, and procedures of the school district, as well as local, state, and federal laws. 5. **Web 2.0 & Web 3.0 Web-based Services** – Certain school district authorized web-based services, such as blogging, authorized social networking sites, wikis, podcasts, RSS feeds, social software, folksonomies and interactive 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 is considered an extension of the classroom and is permitted by the school district.

Students and staff must remember that when using these sites, any speech that is considerate inappropriate in the classroom is in also inappropriate when using these web 2.0 and web 3.0 tools. Students using these tools are reminded to act safely by not disclosing any personal information. Students are reminded that when making comments on these sites, all comments will be monitored by school personnel and if any are thought to be inappropriate they will be deleted immediately.

Internet Safety/Cyberbullying Education

It shall be the responsibility of all members of the Northern Bedford County School District staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the technology department.

The Northern Bedford County School District administrators, teachers, and technology department staff will provide age-appropriate instruction for students who access the Internet through the wired or wireless connections. The instruction provided will be designed to promote the Northern Bedford County School District's commitment to:

1. The standards and acceptable use of Internet services as set forth in this policy;

SC 1303.1-A
47 U.S.C.
Sec. 254
Pol. 249

2. Student safety with regard to:

   a. safety on the Internet;

   b. appropriate behavior while online;

   c. student interactions with other individuals on social networking websites and in chat rooms; and

   d. cyberbullying awareness and response.

3. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Parental Notification And Responsibility

The school district will notify the parents/guardians about the school district's network and the policies governing their use. This policy contains restrictions on accessing inappropriate matter. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the school district to monitor and enforce 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 and matter is and is not acceptable for their child(ren) to access through the school district's network.

Network Etiquette

Users are expected to abide by the generally accepted rules of network etiquette. These include the following:

1. Be polite.

2. Use appropriate language; swearing, vulgarity, and abusive language will not be tolerated. Illegal activities are strictly forbidden.

3. Do not reveal your full name, personal address, phone number or other personally identifiable information or that of any other person.

4. Do not use the network in such a way that you would disrupt the use of the network by other users.

5. All communications and information accessible via the network should be assumed to be district property.

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. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc.

All district computers utilized by students and staff will access the Internet through the content filter that is updated and maintained by the district IT staff.

47 U.S.C. Sec. 254 47 CFR Sec. 54.520	Internet safety measures shall address the following: 1. Control of access by minors to inappropriate matter on the Internet. 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. 6. Restriction of access to visual depictions that are obscene, child pornography or, harmful to minors. <u>Prohibitions</u> Users are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited: 1. Illegal activity. 2. Commercial or for-profit purposes. 3. Non-work or non-school related work. 4. Product advertisement or political lobbying. 5. Hate mail, discriminatory remarks, and offensive or inflammatory communication. 6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
Pol. 237	7. Accessing, sending, receiving, transferring, viewing, sharing, or downloading obscene, pornographic or child pornography, lewd, or otherwise illegal materials, images, or photographs.

	8. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
	9. Inappropriate language or profanity.
	10. Transmission of material likely to be offensive or objectionable to recipients.
	11. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
	12. Impersonation of another user, anonymity, and pseudonyms.
Pol. 814	13. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
	14. Loading or using of unauthorized games, programs, files, or other electronic media, onto a public computer or the network.
	15. Disruption of the work of other users.
	16. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
	17. Quoting of personal communications in a public forum without the original author's prior consent.
	18. Attempt to circumvent any security system or filter employed by the district, including the use of websites or proxy servers to tunnel around firewalls and filtering software, or utilizing the District network or Internet to circumvent any school policy.
SC 1303.1-A Pol. 249	19. Bullying/Cyberbullying another individual or entity. (See school district bullying policy 249.
	20. Accessing the Internet, district computers or other network resources without authorization.
	21. Accessing, sending, receiving, transferring, viewing, sharing, or downloading confidential information without authorization.

	Security Security on any computer system is a high priority, especially when the system involves many users. Attempts to logon to the Internet in any other way than as permitted will result in cancellation of user privileges, disciplinary action, and possible further penalties. System security 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 the system, the following guidelines shall be followed: 1. Employees and students shall not reveal their passwords to another individual. 2. Users are not to use a computer that has been logged in under another student's or employee's name. 3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network. Plagiarism/Copyright/Licensing
17 U.S.C. Sec. 101 et seq Pol. 814	Plagiarism is the act of using someone else's words or ideas as your own. Students and staff are required to properly cite all resources and Internet sites when used in any presentation or assignment, whether quoted or used in entirety. This includes all media files (video and audio), graphics, images, music, text, etc whether found on the Internet or not. In addition all students and staff should follow the copyright laws of the United States (P.L. 94-553) and the Congressional Guidelines that delineate it regarding software, authorship, and copying information. The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines. Also all students and staff should follow the Creative Commons licenses where an author/artists states what media can be shared, remixed, or reused. District Web Site The district shall establish and maintain a website and shall develop and modify its web pages to present information about the district under the direction of the Superintendent or designee. All users publishing content on the district website shall comply with this and other applicable district policies.

	Users shall not copy or download information from the district website and disseminate such information on unauthorized web pages without authorization from the building principal. <u>Consequences For Inappropriate Use</u> The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations; and theft of services will be reported to the appropriate legal authorities for possible prosecution. General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use. Vandalism will result in cancellation of access privileges, disciplinary action and possible further penalties. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.
Pol. 218, 233, 317, 417, 517	Failure to comply with this policy or inappropriate use of the Internet, district network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings. References: School Code – 24 P.S. Sec. 1303.1-A PA Crimes Code – 18 Pa. C.S.A. Sec. 5903, 6312 Child Internet Protection Act – 24 P.S. Sec. 4601 et seq. U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq. Sexual Exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256 Enhancing Education Through Technology Act – 20 U.S.C. Sec. 6777

	Internet Safety, Children's Internet Protection Act – 47 U.S.C. Sec. 254 Children's Internet Protection Act Certifications, Title 47, Code of Federal Regulations – 47 CFR Sec. 54.520 Board Policy – 103, 103.1, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 417, 448, 517, 548, 814, 815.1