

| | |
|---|--|
| <p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p> | <p>The term harmful to minors is defined under both federal and state law.</p> <p>Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that:</p> <ol style="list-style-type: none"> 1. Taken as a whole with respect to minors, appeals to a prurient interest in nudity, sex or excretion; 2. Depicts, describes or represents in 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 lewd exhibition of the genitals; and 3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors. |
| <p>18 Pa. C.S.A. Sec. 5903</p> | <p>Harmful to minors - under state law, is any depiction or representation in whatever form of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:</p> <ol style="list-style-type: none"> 1. Predominantly appeals to the prurient, shameful, or morbid interest of minors; 2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and 3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors. |
| <p>18 Pa. C.S.A. Sec. 5903</p> | <p>Obscene - any material or performance, if:</p> <ol style="list-style-type: none"> 1. The average person applying contemporary community standards would find that the subject matter 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. |
| <p>47 U.S.C. Sec. 254</p> | <p>Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.</p> |

| | |
|---|--|
| | <p>The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.</p> |
| <p>47 U.S.C. Sec. 254</p> | <p>The Board establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors:</p> <ol style="list-style-type: none"> 1. Defamatory. 2. Lewd, vulgar or profane. 3. Threatening. |
| <p>Pol. 103, 103.1, 104, 248, 348</p> | <ol style="list-style-type: none"> 4. Harassing or discriminatory. |
| <p>Pol. 249</p> | <ol style="list-style-type: none"> 5. Bullying. |
| <p>Pol. 218.2</p> | <ol style="list-style-type: none"> 6. Terroristic. |
| | <ol style="list-style-type: none"> 7. Pornographic. |
| <p>24 P.S. Sec. 4604 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p> | <p>The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access.</p> |
| <p>24 P.S. Sec. 4604</p> | <p>Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.</p> |
| <p>24 P.S. Sec. 4610 20 U.S.C. Sec. 6777</p> | <p>Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.</p> |

| | |
|---|---|
| <p>47 U.S.C. Sec. 254</p> <p>4. Delegation of Responsibility</p> <p>24 P.S. Sec. 4604</p> | <p><u>Restrictions</u></p> <p>The Board establishes that network use is a privilege not a right; inappropriate, unauthorized and illegal use will result in cancellation of these privileges and appropriate disciplinary action. The administration, faculty and staff of New Brighton Area School District may request the system administrator to deny, revoke or suspend specific users.</p> <p>The district shall make every effort to ensure that this resource is used responsibly by students and staff.</p> <p>The district shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the district website and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.</p> <p>Users of district networks or district-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the district uses monitoring systems to track and recover lost or stolen equipment.</p> <p>Student user agreements shall also be signed by a parent/guardian.</p> <p>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, and to evaluate and use the information to meet their educational goals.</p> <p>Students, staff and other authorized individuals have the responsibility to respect and protect the rights of every other user in the district and on the Internet.</p> <p>The building administrator shall make the initial determination of whether inappropriate use has occurred.</p> |
|---|---|

| | |
|--|--|
| <p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 CFR Sec. 54.520</p> | <p>The Superintendent or designee shall be responsible for implementing technology and procedures to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:</p> <ol style="list-style-type: none"> 1. Utilizing a technology protection measure that blocks 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 Board. 2. Maintaining and securing a usage log. 3. Monitoring online activities of minors. |
| <p>47 U.S.C. Sec. 254</p> | <p>The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:</p> <ol style="list-style-type: none"> 1. Interaction with other individuals on social networking web sites and in chat rooms. 2. Cyberbullying awareness and response. |
| <p>SC 1303.1-A Pol. 249</p> | |
| <p>5. Guidelines</p> | <p>Network accounts shall be used only by the authorized owner of the account for its approved purpose. Network users shall respect the privacy of other users on the system.</p> <p>Internet Network Access for all users.</p> <p>Internet/Network Access for all users – students and staff.</p> <p>NBASD staff and students will have the opportunity to access Internet services after review of the Acceptable Use Policy and submission of the User/Agreement Form. NBASD staff and student members must maintain proper Internet practices to retain Internet privileges. NBASD staff and students will have access to the Internet and use network resources (including email) for educational purposes only and their usage will be logged.</p> <p><u>Netiquette</u></p> <p>Users are expected to abide by the generally accepted rules of network etiquette.</p> |

| | |
|--|---|
| <p>47 U.S.C. Sec. 254 47 CFR Sec. 54.520</p> | <p><u>Safety</u></p> <p>It is the district’s goal to protect users of the network from harassment and unwanted or unsolicited electronic communication. 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, e-mail, social networking websites, etc.</p> <p>Internet safety measures shall effectively address the following:</p> <ol style="list-style-type: none">1. Control 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 minor’s access to materials harmful to them. <p><u>Supervision And Monitoring</u></p> <p>School and network administrators and their authorized employees monitor the use of information and technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use and disclose any data found on the school’s information networks in order to further the health, safety, discipline and/or security of any student or other person or to protect property. They may also use this information in disciplinary actions and will furnish evidence of crime to school officials and law enforcement.</p> <p><u>Prohibitions</u></p> <p>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:</p> <ol style="list-style-type: none">1. Facilitate any illegal activity including “hacking”. |
|--|---|

| | |
|----------|---|
| Pol. 237 | <ol style="list-style-type: none">2. Commercial or for-profit purposes.3. Nonwork or nonschool related work.4. Product advertisement or political lobbying.5. Harassment, hate mail, discriminatory remarks, and offensive or inflammatory communication.6. Access to obscene or pornographic material or child pornography.7. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.8. Destruction, modification, abuse or unauthorized access to network hardware, software and files.9. Unauthorized or illegal installation, downloading, distribution, reproduction, or use of copyrighted materials.10. Accessing, sending, receiving, transferring, viewing, sharing, or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.11. Use of inappropriate language or profanity.12. Use of the network and/or its resources to transmit material likely to be offensive or objectionable to recipients, including but not limited to spam.13. Intentionally obtaining or modifying files, passwords and data belonging to other users, internal or external to the district's network. |
| Pol. 814 | <ol style="list-style-type: none">14. Fraudulent copying, communication or modification of materials in violation of copyright laws.15. Copying, loading or use of unauthorized or pirated games, programs, files, data or other electronic media.16. Disrupt the work of other users.17. Destruction, modification, vandalism or abuse of network or unauthorized access to network hardware, software, and/or functionality. |

| | |
|---------------------------------|--|
| <p>SC 1303.1-A Pol. 249</p> | <p>18. Quoting of personal communications in a public forum without the original author's prior consent.</p> <p>19. The creation of links to other networks whose content or purpose would tend to violate these guidelines.</p> <p>20. Attaching rogue devices or applications to district resources.</p> <p>21. Sending unsolicited email for the purpose of advertisement or nondistrict business.</p> <p>22. Installation and/or use of nondistrict authorized remote desktop or other computing utilities.</p> <p>23. The use of external hard drives for flash drives on the network.</p> <p>24. Bullying/Cyberbullying.</p> <p>25. Impersonation of another user, anonymity and pseudonyms.</p> <p>26. Accessing the Internet, district computers or other network resources without authorization.</p> <p>27. Disabling or bypassing the Internet blocking/filtering software without authorization.</p> <p>28. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.</p> <p><u>Security</u></p> <p>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:</p> <ol style="list-style-type: none">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. |
|---------------------------------|--|

| | |
|---|--|
| <p>17 U.S.C. Sec. 101 et seq Pol. 814</p> | <p><u>Copyright</u></p> <p>The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines and applicable laws and regulations.</p> <p><u>District Website</u></p> <p>The district shall establish and maintain a web site 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 web site shall comply with this and other applicable district policies.</p> <p>Users shall not copy or download information from the district web site and disseminate such information on unauthorized web pages without authorization from the building principal.</p> |
| <p>24 P.S. Sec. 4604</p> | <p><u>Consequences For Inappropriate Use</u></p> <p>The network user shall be responsible for damages to the equipment, systems and software resulting from deliberate or willful acts.</p> <p>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.</p> <p>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.</p> <p>Vandalism shall result in loss of access privileges, disciplinary action and/or legal proceedings. 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.</p> |
| <p>Pol. 218, 233, 317</p> | <p>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.</p> <p>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.</p> |

Errors/Omission Risks

New Brighton Area School District makes no warranties of any kind, whether expressed or implied, for the service it is providing. New Brighton Area School District will not be responsible for any damages users suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by its own negligence, malfunctions, or user errors or omissions. New Brighton Area School District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Exception Of Terms/Conditions

All terms and conditions as stated in this document are applicable to the New Brighton Area School District. These terms and conditions reflect the entire agreement of the parties and conditions shall be governed and interpreted in accordance with the laws of the Commonwealth of Pennsylvania and the United States of America.

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, 814