

# NEW CASTLE AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF  
INTERNET, COMPUTERS, AND  
NETWORK RESOURCES

ADOPTED: July 14, 2004

REVISED: May 11, 2005, Feb, 21, 2007  
Aug. 24, 2009, Aug. 11, 2010,  
*August 17, 2015*

<p>1. Purpose</p>	<p style="text-align: center;">815. ACCEPTABLE USE OF INTERNET, COMPUTERS, AND NETWORK RESOURCES</p> <p>The Board of Directors of the New Castle Area School District supports the use of the computers, Internet and other network resources in the District's instructional and operational programs in order to facilitate learning, teaching, and daily operations through interpersonal communications and access to information, research, and collaboration.</p>
-------------------	---

<p>2. Definitions</p> <p>18 U.S.C. Sec. 2256</p>	<p>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.</p> <p>For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the New Castle Area School District as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.</p> <p>The term child pornography is defined under both federal and state law.</p> <p>Child pornography – under federal law, is 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:</p> <ol style="list-style-type: none"> <li>1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;</li> <li>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</li> <li>3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.</li> </ol>
--	---

<p>18 Pa. C.S.A. Sec. 6312</p>	<p>Child pornography – under state law, is 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.</p>
<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"> <li>1. Taken as a whole, with respect to minors, appeals to a prurient interest in Nudity, sex, or excretion;</li> <li>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 lewd Exhibition of the genitals; and</li> <li>3. Taken as a whole lacks serious literary, artistic, political, or scientific Value as to minors.</li> </ol>
<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"> <li>1. Predominantly appeals to the prurient, shameful, or morbid interest of Minors;</li> <li>2. Is patently offensive to prevailing standards in the adult community as a whole With respect to what is suitable for minors; and</li> <li>3. Taken as a whole lacks serious literary, artistic, political, educational, or Scientific value for minors.</li> </ol>
<p>18 Pa. C.S.A. Sec. 5903</p>	<p>Obscene – any material or performance, if:</p> <ol style="list-style-type: none"> <li>1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;</li> <li>2. Is patently offensive to prevailing standards in the adult community as a Whole with respect to what is suitable for minors; and</li> <li>3. Taken as a whole lacks serious literary, artistic, political, educational, or scientific value for minors.</li> </ol>

<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>2. Authority</p>	<p>The availability of access to electronic 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. 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.</p> <p>The District shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.</p>
<p>Pol. 218, 233, 317</p>	<p>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, 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 filespace 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, local, state, and federal officials in any investigation concerning or related to the misuse of the District’s Internet, computers, and network resources.</p> <p>The Board requires all users to fully comply with the 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 list of materials, in addition to those stated in law, and defined in this policy, that are inappropriate for access by minors:</p>
<p>Pol. 103, 103.1 104, 248, 348</p>	<ol style="list-style-type: none"> <li>1. Defamatory,</li> <li>2. Lewd, vulgar, or profane</li> <li>3. Threatening</li> <li>4. Harassing or discriminatory</li> </ol>
<p>Pol. 249 Pol. 218.2</p>	<ol style="list-style-type: none"> <li>5. Bullying</li> <li>6. Terroristic</li> </ol>
<p>24 P.S. Sec. 4604 20 U.S.C. Sec. 6777 47 U.S.C.</p>	<p>The District reserves the right to restrict access to any Internet sites or functions it deems in appropriate 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 in appropriate matter by minors on its computers used and accessible to adults and students. The technology</p>

815. ACCEPTABLE USE OF INTERNET, COMPUTERS, AND NETWORK RESOURCES - Pg. 4

<p>Sec. 254</p> <p>24 P.S. Sec. 4604</p> <p>3. Delegation of Responsibility</p> <p>24 P.S. Sec. 4604</p> <p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 CFR Sec. 54.520</p>	<p>protection measure shall be enforced during use of computers with Internet access.</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 materials that is blocked through technology protection measures but is not prohibited by this policy.</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 web site, 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 monitor and detect inappropriate use and tracking 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 discern 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 initial determinations of whether inappropriate use has occurred.</p> <p>The Superintendent or designee shall be responsible for recommending technology and developing procedures to determine whether the District's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to:</p> <ol style="list-style-type: none"> <li>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.</li> </ol>
---	---

<p>47 U.S.C. Sec. 254</p> <p>SC 1301.1-A Pol. 249</p> <p>4. Guidelines</p> <p>47 U.S.C. Sec. 254 47 CFR Sec. 54.520</p>	<ol style="list-style-type: none"> <li>2. Maintaining and securing a usage log.</li> <li>3. Monitoring online activities of minors.</li> </ol> <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"> <li>1. Interaction with other individuals on social networking web sites and in chat Rooms.</li> <li>2. Cyber bullying awareness and response.</li> </ol> <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><u>Safety</u></p> <p>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, e-mail, Internet, social networking web sites, etc.</p> <p>The School District, through the use of a firewall and related software, will filter Internet access pursuant to the Children's Internet Protection Act. The Filter may be disabled by the network administrator at the workstation level for use by an adult, administrator, or teacher for bona fide research or other lawful purposes. The Filter may not be disabled for use by students or other minors for any reason.</p> <p>Internet safety measures shall effectively address the following:</p> <ol style="list-style-type: none"> <li>1. Control of access by minors to inappropriate matter on the Internet.</li> <li>2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.</li> <li>3. Prevention of unauthorized online access by minors, including “hacking” and other unlawful activities.</li> <li>4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.</li> </ol>
---	--

<p>SC 1301.1-A Pol. 249</p> <p>Pol. 237</p> <p>Pol. 814</p>	<p>5. Restriction of minors’ access to materials harmful to them.</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"> <li>1. Facilitating illegal activity.</li> <li>2. Commercial or for-profit purposes.</li> <li>3. Non-work or non-school related work.</li> <li>4. Product advertisement or political lobbying.</li> <li>5. Bullying/Cyber bullying</li> <li>6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.</li> <li>7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.</li> <li>8. Accessing, sending, receiving, transferring, viewing, sharing, or downloading obscene, pornographic, lewd, or otherwise illegal materials, images, or photographs.</li> <li>9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.</li> <li>10. Inappropriate language or profanity.</li> <li>11. Transmission of material likely to be offensive or objectionable to recipients.</li> <li>12. Intentional obtaining or modifying of files, passwords, and data belonging to other users.</li> <li>13. Impersonation of another user, anonymity, and pseudonyms.</li> <li>14. Fraudulent copying, communications, or modification of materials in violation of copyright laws.</li> <li>15. Loading or using of unauthorized games, programs, files, or other electronic media.</li> </ol>
---	---

	<p>16. Disruption of the work of other users.</p> <p>17. <b><i>Tampering with, willful destruction of, or theft of any computer equipment, whether it belongs to the school or to an individual. Tampering includes any deliberate effort to degrade or heal a system,, to tie up a system, or to compromise the system/network performance. Willful destruction includes any deliberate disabling or damaging or computer systems, peripheral equipment, such as scanners or printers, or other facilities or equipment including the network and any deliberate destruction or impairment of software or other users' files or data.</i></b></p> <p>18. Accessing the Internet, District computers, or other network resources without authorization.</p> <p>19. Disabling, or bypassing the Internet blocking/filtering software without authorization.</p> <p>20. Accessing, sending, receiving, transferring, viewing, sharing, or downloading confidential information without authorization.</p> <p>21. Quoting of personal communications in a public forum without the original author's prior consent.</p> <p>22. <b><i>The use of cameras in private places. A private place is one where a person may reasonably expect to be safe from unauthorized surveillance, such as locker rooms, restrooms, etc.</i></b></p> <p>23. <b><i>Geo-location or Geo Tagging services are prohibited on District property. Broadcasting your location or the location of others is not allowed. This supports privacy and security efforts within the District.</i></b></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"><li>1. Employees and students shall not reveal their passwords to another individual.</li><li>2. Users are not to use a computer that has been logged in under another student's or employee's name.</li></ol>
--	---

<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 Web-Site</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><u>Consequences For Inappropriate Use</u></p>
<p>24 P.S. Sec. 4604</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.</p> <p>Vandalism shall result in loss of access, 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>References:</p> <p>School Code – 24 P.S. Sec. 1303.1-A</p> <p>PA Crimes Code – 18 Pa. C.S.A. Sec. 5903, 6312</p> <p>Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.</p>



	<p>U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq.</p> <p>Sexual exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256</p> <p>Enhancing Education Through Technology Act – 20 U.S.C. Sec. 6777</p> <p>Internet Safety, Children’s Internet Protection Act – 47 U.S.C. Sec. 254</p> <p>Children’s Internet Protection Act Certifications, Title 47, Code of Federal Regulations – 47 CFR Sec. 54.520</p> <p>Board Policy – 103, 103.1, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 814</p>
--	--