



Network and Internet Access Agreement for Students

- Any student age 18 and older is to read this form (7540.03 F1). Page 5 of this form should then be completed and returned to the Building Library/Media Specialist.
- Any student under age 18 and their parent/guardian is to read this form (7540.03 F1). Page 5 of this form should then be completed and returned to the Building Library/Media Specialist.
- Users shall not be granted access to the Network until they have turned in the completed page 5 of this form.

Advances in telecommunications and other related technologies have fundamentally altered the ways in which information is accessed, communicated, and transferred in society. The Board of Education is pleased to provide Internet services to its students. The District's Internet system has a limited educational purpose. The District's Internet system has not been established as a public access service or a public forum. The Board has the right to place restrictions on its use to assure that use of the District's Internet system is in accord with its limited educational purpose. Student use of the District's computers, network and Internet services ("Network") will be governed by this policy and the related administrative guidelines, and the Student Code of Conduct. The due process rights of all users will be respected in the event there is a suspicion of inappropriate use of the Network. Users have no right or expectation to privacy when using the Network (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity while on the Network).

Students are encouraged to use the Board's computers, network, and Internet connection ("Network") for educational purposes. Use of the Network is a privilege, not a right. When using the Network, students must conduct themselves in a responsible, efficient, ethical, and legal manner. Users who disregard this policy may have their use privileges suspended or revoked, and disciplinary action taken against them. Users granted access to the Internet through the Board's computers assume personal responsibility and liability, both civil and criminal, for uses of the Internet not authorized by this Board policy. Prior to accessing the Network students must sign the Student Network and Internet Acceptable Use and Safety Agreement. Parent permission is required for minors.

Smooth operation of the Board's Network relies upon users adhering to the following guidelines. The guidelines outlined below are not exhaustive, but are provided so that users are aware of their general responsibilities.

In exchange for the use of the Network resources, either on-site or by remote access, the user understands and agrees to the following:

- A. Privilege:** The use of Network is a privilege which may be revoked by the District at any time and for any reason.
- B. Scope of Acceptable Use:** Network resources shall be used for the purposes of (in order of priority):
 1. supporting the academic program;
 2. telecommunications;
 3. general information.

The District periodically may make determinations on whether other incidental non-educational uses of the Network are consistent with this Agreement. Uses that interfere with normal District business or educational activities are prohibited and may be cause for disciplinary action at the discretion of the District. It is within the rights of the District to periodically modify the list of acceptable use.

Pursuant to Federal law, the Board has implemented technology protection measures, which protect against (e.g. filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act. At the discretion of the Board or the Superintendent, the technology protection measures may be configured to protect against access to other material considered inappropriate for students to access. Any student who attempts to disable the technology protection measures will be subject to discipline.

The Superintendent or his/her designee may temporarily or permanently unblock access to sites containing appropriate materials, if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures.

The District shall monitor the user's online activities, through direct observation and/or technological means, to endeavor to ensure that users are not accessing such depictions or any other materials that are inappropriate for the educational setting. To the extent practical, steps shall also be taken to promote the safety and security of users when utilizing e-mail, chat rooms, instant messaging and other forms of direct electronic communication.

Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines.

Staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified below. Furthermore, staff members will monitor the online activities of students while at school.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; or use of specific monitoring tools to review browser history and network, server, and computer logs.

Pursuant to Federal law, students shall receive education about the following:

1. safety and security while using e-mail, chat rooms, social media, and other forms of direct electronic communications;
2. the dangers inherent with the online disclosure of personally identifiable information;
3. the consequences of unauthorized access (e.g., "hacking") cyberbullying and other unlawful or inappropriate activities by students online, and
4. unauthorized disclosure, use, and dissemination of personal information regarding minors

- C. Access:** Selected Network resources are intended only for the use by their registered users who agree to abide by this Agreement. Users shall not share their password(s) with others or otherwise allow anyone unauthorized access to the Network. A user is responsible for any violations of this agreement committed by someone who, with the user's express or implied permission, accessed the network with the user's password. Students may use the Network only under the supervision of a staff member.

Students may use real-time electronic communication, such as chat or instant messaging, only under the direct supervision of a teacher or in moderated environments that have been established to support educational activities and have been approved by the Board, Superintendent, or building principal.

Students shall not access social media for personal use from the District's network, but shall be permitted to access social media for educational use in accordance with their teacher's approved plan for such use.

Students may not establish web-based e-mail accounts on commercial services through the Network (e.g., Gmail, Hotmail, Yahoo mail).

Preservation of Resources and Priorities of Use: Computer resources are limited. Because space on disk drives and bandwidth across the lines which connect the Network (both internally and externally) are limited, neither programs nor information may be stored on the system without the permission of the Chief Technology Officer. Each student is permitted reasonable space to store e-mail, web, and personal files. The Board reserves the right to require the purging of files in order to regain disk space. Students who require access to the Network for class- or instruction-related activities have priority over other users. Students not using the Network for class-related activities may be "bumped" by any student requiring access for class- or instruction-related purpose.

Non-educational game playing is not permitted at any time.

D. Network Etiquette: Use of the Network has great potential to enhance the productivity of the users. The Network, however, could also be abused. User shall be held accountable for their use or misuse of the Network. Each user must abide by generally accepted rules of Network etiquette, which include but are not limited to:

1. Users shall not obtain copies of, or modify files, other data, or passwords belonging to other users without express authorization.
2. Users shall not misrepresent themselves on the Network.
3. Users shall not use the Network in any way that would disrupt the operation of the Network; abuse the software and/or hardware; or excessively consume limited computer, paper or telephone resources, such as through spamming, creating or forwarding mass e-mails, sending chain letters, or extensively using the Network for non-curriculum-related communications or other purposes exceeding the Scope Of Acceptable Use under this agreement.
4. Users shall not create or transmit harassing, threatening, abusive, defamatory or vulgar messages or materials.
5. Users shall not reveal any personal information beyond directory information about themselves, other students, or District employees, including social security numbers, passwords, etc.
6. Users shall not create, transmit, or download any materials (a) that are in violation of District Policies or any state or federal law, including but not limited to confidential information, copyrighted materials, material protected by trade secrets, and any materials that would violate the District's Harassment Policy; or (b) that include the design or detailed information for the purposes of creating an explosive device, materials in furtherance of criminal activities or terrorist acts, threatening materials, or pornographic, sexually explicit or obscene materials.

7. Users shall not use the Network for any commercial activities, such as buying, advertising or selling goods or services, unless doing so is pre-approved by the District. The District shall not be liable for any transactions, costs, damages or fees incurred by a user through purchases of goods or services or other transactions through the Network, or for any illegal actions, including copyright violations, that a user performs through the Network.
8. Users shall not use or install any software or program not already on district equipment unless authorized by a district administrator.
9. Users shall not engage in cyberbullying. "Cyberbullying is the use of technology to harass, threaten, embarrass, or target another person."
(<http://kidshealth.org/parent/positive/talk/cyberbullying.html>)

Cyberbullying includes, but is not limited to the following:

1. posting slurs or rumors or other disparaging remarks about a student on a website or blog;
2. sending e-mail, instant messages, or text messages that are mean or threatening, or so numerous as to drive up the victim's cell phone bill;
3. using a camera or phone to take and send embarrassing and/or sexually explicit photographs/recordings of students;
4. posting misleading or fake photographs of students on web

- E. Web Sites:** Web sites created for school community organizations through the Network or linked to District's web site must relate specifically to officially sanctioned organization activities and programs. The District reserves the right to require that material and/or links to other sites found to be objectionable be altered or removed.

Proprietary rights in the design of websites hosted on the Board's servers remains at all times with the Board.

- F. Service Disclaimer:** The District does not warrant that the functions of the Network will meet any specific requirements the user may have, or that the Network will be error free or uninterrupted; nor shall the District be liable for any direct or indirect, incidental, or consequential damages (including lost data, information, or time) sustained or incurred in connection with the use, operation or inability to use or operate the system.

- G. Reservation Of Rights:** The District administrators and/or Network managers may perform the following actions for any legitimate reason, including but not limited to for the purposes of maintaining system integrity and insuring that users are using the Network consistently with this Agreement: monitor, inspect, copy, review, and store at any time and without prior notice any and all usage of the Network and any and all materials, files, information, software, communications, and other content transmitted, received or stored in connection with this usage. The District reserves all rights to any material stored in files which are generally accessible to others and will remove any materials which the District, at its sole discretion, believes may be unlawful, obscene, pornographic, abusive, or otherwise objectionable. The Network and all information, content, and files contained therein are the property of the District, and users should not have any expectation of privacy regarding those materials.

- H. File Transfers:** A user may not transfer files, shareware or other software from information services and electronic bulletin boards without prior authorization of the District staff. The user may be liable to pay the cost or fee of any unauthorized file, shareware, or software transferred, whether intentionally or accidentally. For each file received through a file transfer, the user must check the file with a virus-detection program before opening the file for use.
- I. Vandalism:** Vandalism is prohibited. For the purpose of this Agreement, vandalism is any malicious attempt to harm or destroy software, hardware, data of another user, other Network resources, or the use of the Network to harm or destroy anything on the Internet or outside networks. Vandalism includes but is not limited to the uploading, downloading, creating or transmitting of computer viruses, worms, Trojan horses, or other destructive programs or applications. Should the user cause the Network to become infected with a virus or other destructive program or application and the infection causes damage to the Network, the user may be liable for any and all repair costs to restore the Network to full operational status in addition to other potential disciplinary measures as determined by the District.
- J. Security:** If a user identifies a security problem with the Network, the user must notify a Network administrator, teacher, or building principal immediately. Users must report all activities that are illegal or in violation of District Policies to a teacher or building principal. All users agree to cooperate with the District in the event of an investigation into any allegations of misuse or security breaches of the Network.
- K. Use of Wireless Communication Devices (WCDs):** In accordance with Policies 5136, 5136.01, and Administrative Guideline 5136, students using personal WCDs are to follow all rules as established and only connect or attempt to connect to networks designated for student use.
- L. Violations Of This Policy:** Any violations of this Policy may result in disciplinary action, including but not limited to restriction or termination of access to the Network, other discipline in accordance with the Student Code of Conduct, referral to legal authorities, and/or other legal action. Users granted access to the Internet through the Board's computers assume personal responsibility and liability, both civil and criminal, for uses of the Internet not authorized by this Board policy and its accompanying guidelines.

The Board designates the Superintendent and Chief Technology Officer as the administrators responsible for initiating, implementing, and enforcing this policy as it applies to students' use of the Network.

THIS PAGE INTENTIONALLY BLANK



Network and Internet Access Agreement Form for Students

- Any student age 18 and older is to read this form (7540.03 F1). Page 5 of this form should then be completed and returned to the Building Library/Media Specialist.
- Any student under age 18 and their parent/guardian is to read this form (7540.03 F1). Page 5 of this form should then be completed and returned to the Building Library/Media Specialist.
- Users shall not be granted access to the Network until they have turned in the completed page 5 of this form.

Teacher's Name _____ Homeroom _____

Student Name (Print) _____

In consideration for the privilege of accessing the Network, and in consideration for having access to the information contained on the Network, or by the Network, I hereby release the District, its administration and Network operators from any and all claims of any nature arising from my use, or inability to use, Network resources. I also understand that while my Network use may be monitored, and filters are used for Internet access, I am still responsible for my use of the Network and understand that I am required to avoid sites that are inappropriate for the educational setting.

I have agreed that I have read, understood and will abide by these rules and regulations of Network usage and any additional rules that may be added from time to time by the District.

(Sign and return to Building Library Media Specialist.)

Signature of Student

Grade Level

Date

If the student is under the age of 18, a parent/guardian must complete the following:

As the student's parent or legal guardian, I grant permission for my child to use the Network. I further agree that I have read and understand this agreement and will indemnify the District for any fees, expenses, or damages incurred as a result of my child's use or misuse of the Network or equipment.

Signature of Parent/Guardian

Date