Authorization for Electronic Network Access

In order for a District staff member to gain electronic network and Internet privileges, the staff member must submit a signed copy of the Authorization for Electronic Network Access (Attachment A).

In order for a student to gain electronic network and Internet privileges, the student must submit a copy of the Authorization for Electronic Network Access (Attachment A) with signatures from both the student and the student's parent(s) or guardian(s)

All use of the District's electronic network and the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This *Authorization* does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. The failure of any user to follow the terms of the *Authorization for Electronic Network Access* will result in the loss of privileges, disciplinary action consistent with existing District disciplinary policies, and/or appropriate legal action. The signature(s) at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

Terms and Conditions

1. Acceptable Use – Access to the District's electronic network must be, (a) for the purpose of education or research and be consistent with the educational objectives of the District, or (b) for legitimate business use. Access also must comply with the Policy, these Rules and Regulations, other rules, regulations or other terms or conditions of electronic network access promulgated by the Superintendent or Building Principals, and all other disciplinary policies and regulations necessary for the safety and pedagogical concerns of the District.

2. Privileges – The use of the District's electronic network is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator (superintendent or designee) may deny, revoke, or suspend the access privileges of any user who violates this Authorization or any terms or conditions governing use of the District's electronic network. Additional disciplinary measures, if any, may be considered and imposed consistent with District discipline policies.

3. Unacceptable Use – Any use which disrupts the proper and orderly operation and discipline of schools in the District; threatens the integrity or efficient operation of the District electronic network; violates the rights of others; is socially inappropriate or inappropriate for a student's age or maturity level; is primarily intended as an immediate solicitation of funds; is illegal or for illegal purposes of any kind; or constitutes gross disobedience or misconduct is an unacceptable use. The user is responsible for his or her actions and

activities involving the network. Use of the District electronic network for any unacceptable use will result in the suspension or revocation of electronic network privileges, disciplinary action, and/or appropriate legal action. Unacceptable uses of the District's electronic network specifically include, but are not limited to, the following:

a. Using the network for any illegal activity, such as fraud, (including academic fraud), libel, slander, plagiarism, forgery, or a violation of copyright laws or other intellectual property rights or contracts, or transmitting any material in violation of any federal or State law;

b. Downloading or installing any software, music, video or other media or other file to the District's electronic network without prior permission from the Superintendent, Building Principal, or their designees;

c. Using the network for private financial or commercial gain;

d. Wastefully using resources, such as file space;

e. Hacking or gaining unauthorized access to files, resources, or entities;

f. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, or use of information about anyone that is of a personal nature;

g. Using another user's account or password;

h. Disclosing any electronic network password (including your own) to any other individual;

i. Modifying, disabling, compromising, or otherwise circumventing any anti-virus, user authentication, or other security feature maintained on the District network or on any external computer, computer system, or computer account.

j. Creating or sending e-mail or other communications which purport to come from another individual (commonly known as "spoofing"), or otherwise assuming an anonymous or false identity in communicating with other individuals, businesses, or organizations;

k. Using encryption software or otherwise encoding or password-protecting any file which is created with, sent from, received by, or stored on the District's electronic network;

l. Creating or deliberately downloading, uploading, or forwarding any computer virus, or otherwise attempting to modify, destroy, or corrupt computer files maintained by any individual on any computer;

m. Posting material authorized or created by another without his/her consent;

n. Posting anonymous messages;

o. Using the network for commercial or private advertising;

p. Accessing, submitting, posting, publishing, or displaying any material which is defamatory, abusive, obscene, profane, sexually oriented, threatening, harassing, illegal, or which violates the rights of others;

q. Using the network while access privileges are suspended or revoked; and

r. Attempting to commit any action which would constitute an unacceptable use if accomplished successfully.

4. Network Etiquette – The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

a. Do not become abusive in messages to others.
b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
c. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.

d. Recognize that electronic mail (E-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

e. Do not use the network in any way that would disrupt its use by other users.

f. Consider all communications and information accessible via the network to be private property of the school district.

5. No Warranties – The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the users own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

6. Indemnification –

a. The student and parent agree to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of the student's *Authorization for Electronic Network Access* (Attachment A).

OR

b. The District employee agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of the employee's *Authorization for Electronic Network Access* (Attachment A).

7. Security – Network security is a high priority. If you can identify a security problem on the Internet, you must notify the system administrator or building principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without permission from that individual. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

8. Vandalism – Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

9. Telephone Charges – The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

10. Use of Copyrighted Material From the Internet – Copyright law and District policy prohibit the republishing of text or graphics found on the Internet or on District Web-sites or file servers without explicit written permission.

    a. For each re-publication (on a Web-site or file server) of a graphic or a text file that was produced externally, there must be credit given to the original producer. If possible, the notice should also include the Internet address of the original source.

    b. Students and staff engaged in producing Web pages must provide library media specialists with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.

    c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web-site displaying the material may not necessarily be considered a source of permission.

    d. The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

11. Internet Publishing Guidelines – From time to time, the District may publish student names, student photographs, or material created by students and/or District staff on the District's website consistent with the following guidelines.

    a. Students may be identified on the District's website by first name or first initial only. Under no circumstances shall a student's last name or last initial, home address, telephone number, e-mail address, or other information which would allow a visitor to the District website to personally contact the student be published on the District's website.

b. Under no circumstances shall a student's name appear with a student's photograph or in any other context which would allow a visitor to the District website to associate a student's name with a photograph, image, or likeness of the student.

c. Any material which is published on the District's website must be sponsored by a District employee and approved for publication by the Superintendent, the appropriate Building Principal, or their designee(s).

d. Staff works which are prepared in the scope of employment are works "made for hire" within the meaning of the Copyright Act, 17 U.S.C. § 101 et seq., and all copyrights and other intellectual property rights in and to such works vest in the District. Submission of other staff works for publication on the District's website shall give rise to a non-exclusive, non-transferable license in favor of the District for such publication.

e. Copying or reproduction of text, graphics, sounds, or other material found on the District's website is prohibited without express written permission. Any permitted copying or reproduction must include credit to the District and to the original author.

12. Use of Electronic Mail

a. The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.

b. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. The District may access and disclose account information as necessary to further legitimate District interests. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.

c. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.

d. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this School District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.

e. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator (superintendent or designee). Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.

13. Cooperation with Investigations – The District reserves the right to participate and cooperate fully in any investigation requested or undertaken by either law enforcement authorities or a party alleging to have been harmed by the use of the District electronic network. Evidence of illegal activity may be reported or turned over to appropriate authorities.

14. Enforcement – The failure of any user to abide by the Policy, these Rules and Regulations, or other rules, regulations or other terms or conditions of electronic network access promulgated by the Superintendent or Building Principals will result in the suspension or revocation of the user's electronic network privileges, disciplinary action, and/or appropriate legal action. Electronic network privileges may be suspended or revoked by the Superintendent or Building principal. Disciplinary measures, if any, will be considered and imposed consistent with District discipline policies.

15. Execution of Staff/Student Authorizations

a. **District Staff** – In order for a District staff member to gain electronic network and Internet privileges, the staff member must submit a signed copy of the *Authorization for Electronic Network Access* (Attachment A). If a staff member's electronic network privileges are suspended or revoked, newly-signed copies of the staff authorization must be submitted before the staff member's access privileges are restored. The District may also require that staff members submit newly-signed authorizations as a condition of continued access when necessary to incorporate changes in technology, law, or District policy, or when otherwise determined by the Superintendent or designee to be in the best interests of the District.

b. **Students** – In order for a student to gain electronic network and Internet Privileges, the student must submit a copy of the *Authorization for Electronic Network Access* (Attachment A) with signatures from both the student and the student's parent(s) or guardian(s). If a student's electronic network privileges are suspended or revoked, newly-signed copies of the student and parental authorizations must be submitted before the student's access privileges are restored. Newly-signed student and parental authorizations must also be submitted each time the student enters into a new District school. The District may also require that students submit newly-signed student and parental authorizations as a condition of continued access when necessary to incorporate changes in technology, law, or District policy, or when otherwise determined by the Superintendent or designee to be in the best interests of the District.

16. Policy Modifications – The terms and conditions of use and/or the provisions of this Policy may be modified. Notice of such modifications or additional rules, regulations, or other terms of condition of access shall be promptly communicated to all authorized users, including by posting such modifications on the electronic network or in a conspicuous place at access locations.

<u>Internet Safety</u>

1. Internet access is limited to only those "acceptable uses" as detailed in these procedures. The District's primary concern in maintaining Internet access is that student safety and security not be compromised at any time. The procedures are designed to mitigate potential harms from using the Internet, but the District cannot guarantee that these measures will be completely effective.

2. Staff members shall supervise students while students are using District Internet access and enforce the Terms and Conditions for Internet access contained in this *Authorization*.

3. Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the *Children's Internet Protection Act* and as determined by the Superintendent or designee.

4. The system administrator (Superintendent or designee) and Building Principals shall monitor student Internet access.

5. Some of the most effective safety measures can only be implemented by students themselves. The District encourages parents and guardians to discuss the following safety concerns with their students:

a. Students should not give out such personal information as their name, age, home address, telephone number(s), photograph, their parents' or guardians' work address or telephone number, or the name or location of the school over the Internet or through e-mail. Students should not give out such personal information about other individuals over the Internet or through e-mail. Students should be particularly diligent when using "social networking" sites such as myspace.com, facebook.com and xanga.com.

b. Students should immediately inform their parents, guardians, or a member of District staff if they come across any information on the Internet or in an e-mail that makes them feel uncomfortable. Students should not respond to any e-mail or other message which makes them feel uncomfortable.

c. Students should never agree to meet someone in person whom they have "met" online without parental knowledge, permission, and supervision.

d. Students should never agree to send or accept any item to or from a person whom they have "met" online without parental knowledge, permission, and supervision.

6. The District has acted in good faith and in a reasonable manner in selecting and implementing filtering software, blocking software, and other technology protection measures to prevent access to material which is obscene, pornographic, or with respect to use of computers by minors, harmful to minors. Nevertheless, by using the District's electronic network, users acknowledge that such technology measures do not prevent access to all prohibited material, and may prevent access to non-prohibited material. The District assumes no responsibility for access gained or denied by the technology protection measures that have been implemented.

Authorization For Electronic Network Access

I understand and will abide by the above *Authorization for Electronic Network Access* and Board Policy 6:235. I understand that the District and/or its agents may access and monitor my use of the Internet, including my E-mail and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the District's electronic network connection and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the Electronic Network.

DATE: _____

_____

USER SIGNATURE

(Signature below required if the user is a student:)

I have read this *Authorization for Electronic Network Access* and Board Policy 6:235. I understand that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District and/or its agents to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed the terms and content of this *Authorization* with my child. I hereby request that my child be allowed access to the District's Electronic Network.

DATE: _____

_____

PARENT/GUARDIAN NAME (Please Print)

SIGNATURE: _____

ATTACHMENT A