

**RULES AND REGULATIONS IMPLEMENTING
BOARD POLICY 6:235**

ACCESS TO ELECTRONIC NETWORKS

I. Scope of Rules and Regulations and School District Authority

These Rules and Regulations are promulgated pursuant to the Access to Electronic Networks Policy (the “Policy”). These Rules and Regulations govern all use of District computers, the District’s local and/or wide area network, and access to the Internet through District computers or the District’s local and/or wide area network, which will be collectively referred to in these Rules and Regulations as the District’s “computer network.”

The Policy and these Rules and Regulations may be supplemented by additional rules, regulations, and other terms and conditions of computer network use that may be promulgated by District staff pursuant to the Policy or these Rules and Regulations.

The goal of the Board is to include appropriate computer network access in the District’s instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication. All use of the District computer network shall conform to the requirements of all District policies. Access to the Internet through the District computer network must be for the purpose of education or research and must be consistent with the educational objectives of the District.

II. Obtaining Authorization to Use Computer Network

A. Authorized Users

Authorized users of the computer network include students, teachers, administrators, other employees of the District, and Board of Education members who have been given access to the network, have submitted the appropriate authorization forms, and whose computer network privileges are not suspended or revoked.

B. Students

To obtain access to the District’s computer network, a student must submit properly signed copies of the Student’s Authorization for Computer Network Access (Exhibit 1, the “Student Authorization”) and the Parental Authorization for Student’s Computer Network Access (Exhibit 2, the “Parental Authorization”). A record of the student’s submission of these forms will be kept in the student database. Copies of these authorizations shall be kept at the school which the student attends. Students will not be permitted to access the Internet through the computer network, however, unless the student’s parent or guardian has signed and submitted the *Parent Authorization for Student Electronic Network Access* form.

Unless a student's computer network privileges have been suspended or revoked, the Student and Parental Authorizations and student ability to access the network will be valid so long as the student attends the school which the student was attending when the access was issued. If a student's computer 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. Upon submission of newly-signed authorizations, the District will renew the student's access to the network.

Any violation of the terms of these Authorizations, of the Policy, of these Rules and Regulations, or of additional rules, regulations, or other terms and conditions of computer network access promulgated by the Superintendent or Building Principals will result in the suspension or revocation of computer network privileges, disciplinary action, and/or appropriate legal action.

C. Non-Student Users

To obtain network access, teachers, other District staff members, volunteers and Board members ("Non-Student Users") must submit a signed copy of the Non-Student Authorization for Computer Network and Internet Access (Exhibit 3, the "Non-Student Authorization").

Unless a Non-Student User's computer network privileges have been suspended or revoked, this authorization will be valid so long as the user remains an employee of the District or a member of the Board of Education. If a Non-Student User's computer network privileges are suspended or revoked, the user must submit a newly-signed Non-Student Authorization before the user's access privileges are restored.

Any violation of the terms of this Authorization, of the Policy, of these Rules and Regulations, or of additional rules, regulations, or other terms or conditions of computer network access promulgated by the Superintendent or Building Principals will result in the suspension or revocation of computer network privileges, disciplinary action, and/or appropriate legal action.

III. Use of Computer Network

A. Acceptable Use

Access to the District computer network is limited to bona fide educational or research purposes consistent with the District's educational mission. Access also must comply with the Policy, these Rules and Regulations, other rules, regulations or other terms or conditions of computer 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.

B. 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 computer 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. Use of the District computer network for any unacceptable use will result in the suspension or revocation of computer network privileges, disciplinary action up to and including expulsion (for students) or termination from employment (for employees), and/or appropriate legal action.

Unacceptable uses of the District's computer network specifically include, but are not limited to, the following:

1. Taking any steps which threaten, or which may reasonably be interpreted to threaten, any person, group of persons, building, or property with harm, regardless of whether the user intends to carry out such threat, including cyber-bullying. (Cyber-bullying is defined as, but is not limited to, harassing, teasing, intimidating, threatening or terrorizing another person by sending or posting inappropriate and harmful e-mail messages, instant messages, text messages, digital pictures, images or video, or web site postings via social networking sites or other electronic means.);
2. Compromising the privacy or safety of other individuals by disclosing personal addresses, telephone numbers, or other personal identifying information;
3. Accessing, using or possessing any material in a manner that constitutes or furthers fraud (including academic fraud), libel, slander, plagiarism, forgery, or a violation of copyright or other intellectual property right or transmitting any material in violation of State or federal law;
4. Using the computer network for commercial, private, or personal financial gain, including gambling;
5. Deliberately accessing, creating, submitting, posting, publishing, transmitting, receiving, displaying, or otherwise possessing or disseminating any material that is defamatory, abusive, obscene, profane, sexually oriented, sexually explicit, perversely lewd and vulgar, threatening, harassing or illegal, including indecent or inappropriate language, text, sounds, or images;

6. Creating or forwarding chain letters, “spam,” or other unsolicited or unwanted messages;
7. Gaining unauthorized access to resources or entities, including, but not limited to, other student files, teacher files, confidential information, student record data, and unauthorized computer network accounts;
8. Coercing 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;
9. 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;
10. Using or accessing another user’s computer network account or password, with or without consent from the user;
11. Downloading or installing text files, images, or other files to the District’s computer network without prior permission from the Superintendent, Building Principal, or their designees;
12. Downloading, installing, or updating software to the District’s computer network without prior permission from the Superintendent, Building Principal, or their designees (Staff requesting the installation of software need to submit the appropriate form to their Technology Facilitator.);
13. 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;
14. Participating in, or subscribing to non school-related mailing lists, newsgroups, chat services, electronic bulletin boards, or any other non-school related association or service which would cause a large number of e-mails or other electronic messages to be sent to the District’s computer network;
15. Using encryption software or otherwise encoding or password-protecting any file which is created with, sent to, received by, or stored on the District’s computer-network;

16. Using the computer network for the purpose of harassing other users or other individuals;

17. For Non-Student Users, using the computer network to participate in acts constituting “prohibited political activities” under the *State Officials and Employees Ethics Act* or “election interference” under the *Election Code*, or to participate in any political activities that create the appearance of impropriety under those laws or under any ethics policy of the District relating to political activities of District employees;

18. Using the network resources, such as file space, in a wasteful manner;

19. For Employees, failure to abide by Board Policy [BOARD POLICY: 5:125], *Electronic Communication & Social Networking*, and its implementing Procedures; and

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

IV. Student Use of the Internet

A. Procedures

Students shall abide by the rules, regulations and procedures implemented by this Policy and their teachers when using the computer network at school.

Student access to the Internet is only allowed under the direct supervision of a teacher, and with specific educational purpose assigned by the teacher. Students in kindergarten through 5th grade may not use Internet search engines without teacher supervision.

B. Internet Safety

The District’s primary concern in maintaining Internet access is that student safety and security may not be compromised at any time. Some of the most effective safety measures can only be implemented by students themselves. The District strongly recommends parents and guardians discuss the following safety concerns with their students:

1. Students should never 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 never give out such personal information about other individuals over the Internet or through e-mail.

2. 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.
3. Students should never agree to meet someone in person whom they have “met” online without parental knowledge, permission, and supervision.
4. 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.

V. Downloads

Users may only download text files, images, or other files or software obtained through the Internet, e-mail, file transfer protocol (ftp), or other means of file-sharing with the permission of the Superintendent, Building Principal, or their designees.

VI. Privacy

Any electronic communications or files created on, stored on, or sent to, from, or via the computer network are the property of the District. Consequently, users do not have any expectation of privacy with respect to such messages and files. Users should remember that such messages and files can be recovered from the computer network’s back-up system even after they have been deleted from a user’s individual account.

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

The Superintendent, Building Principals, and/or their designees may access and review such messages and files when necessary to maintain the integrity and efficient operation of the computer network; to monitor compliance with the Policy, these Rules and Regulations, and all other rules, regulations, or terms or conditions of computer network access promulgated by the Superintendent or designee; and to further all other educational, safety and pedagogical concerns of the District. The District also reserves the right to intercept, access, and disclose to appropriate authorities all information created with, sent to, received by, or stored on the computer network at any time, with or without user notice. Use of the District’s computer network to create, store, send, receive, view, or access any electronic communication or other file constitutes consent by the user for the District to access and review such files consistent with this paragraph.

E-mail accounts which are issued by the District to any user remain the property of the District, and the District reserves the right to disclose the e-mail addresses of accounts issued to Non-Student Users to parents and other members of the public consistent with legitimate District purposes.

VII. Technology Protection Measures

Consistent with the District’s legitimate educational and pedagogical concerns, the District shall implement technology protection measures, which may include filtering and/or blocking software, on every District computer which has access to the Internet.

Such technology protection measures shall be implemented in the best manner practicable to prevent access to any material, including visual depictions, which is obscene; which constitutes pornography, including child pornography, or which, with respect to use of computers by minors, would be harmful to minors, as defined by the *Children's Internet Protection Act*. The Superintendent, Building Principals, or their designees may disable the technology protection measure on an individual computer during use by non-student adults to enable access to material needed for bona fide research or other lawful purpose.

The District shall monitor the use of the computer network by students and any other minor user in order to ensure compliance with the Policy, these Rules and Regulations, other rules, regulations or other terms of conditions of computer network access promulgated by the Superintendent or Building Principals, and other disciplinary policies and regulations necessary to further the educational, safety, and pedagogical concerns of the District.

VIII. Security

The security and integrity of the District's computer network is a high priority. Users are to keep their account and password secure and confidential at all times. If a Student user believes at any time that he or she has identified a security gap, weakness, or breach on the District's computer network or on the Internet, the user must notify a District staff member immediately. If a Non-Student user believes that he or she has identified a security gap, weakness, or breach on the District's computer network or on the Internet, the user must notify the Building Principal immediately. The user may not exploit the gap, weakness, or breach, and the user may not inform any other individuals of it.

Any user who violates this procedure may be subject to a suspension or revocation of computer network privileges, disciplinary action, and/or appropriate legal action.

IX. No Warranties

A. The District makes no warranties of any kind, whether express or implied, for the service of providing computer network access to its users, and bears no responsibility for the accuracy or quality of information or services obtained from the computer network or any loss of data suffered in connection with use of the computer network. The District will not be responsible for any damages any user suffers, including loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by users' errors, omissions, or negligence. Use of any information obtained from the computer network is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through the computer network.

B. 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, relating to, or arising out of, an individual user's use of the computer network.

C. 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 computer 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.

X. Indemnification

The user agrees to indemnify the District for any losses, costs, damages, charges or fees, including, but not limited to, telephone charges, long-distance charges, per-minute surcharges, equipment or line costs, or attorney fees, incurred by the District and relating to, or arising out of the user's use of the District's computer network or any violation by the user of the Policy, these Rules and Regulations, or other rules, regulations or other terms or conditions of computer network access promulgated by the Superintendent or designee.

XI. 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 computer network. Evidence of illegal activity shall be reported or turned over to appropriate authorities.

XII. 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 computer network access promulgated by the Superintendent or Building Principals will result in the suspension or revocation of the user's computer network privileges, disciplinary action, and/or appropriate legal action. Computer 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. Discipline may include dismissal for Non-Student Users or expulsion for Student Users.

XIII. Policy Modifications

The Board of Education or its designee may modify the terms and conditions of use and/or the provisions of this Policy and its implementing Rules and Regulations at any time. The Superintendent or Building Principals may also promulgate additional rules, regulations, or other terms or conditions of computer network access as may be necessary to ensure the safe, proper, and efficient operation of the computer network and the individual District schools. Notice of any such modifications or additional rules, regulations, or other terms or conditions of access shall be promptly communicated to all authorized users, including by posting such modifications on the computer network or in a conspicuous place at access locations. Use of the computer network constitutes acceptance of the terms of the Policy, these Rules and Regulations, and any additional rules, regulations, or other terms or conditions of computer network access which may have been promulgated by the Superintendent, Building Principals, or their designees.

Exhibit 1

Student's Authorization For Electronic Network Access

I have read, or have had explained to me, the attached Policy and procedures regarding the use of the School District's electronic network, and I agree that I will follow these rules when I use the District's electronic network. I understand that, if I use the District's electronic network in a way that violates these rules, I can be disciplined. Discipline may include loss of electronic network use privileges, detention, suspension, expulsion or other consequences. I understand that any information or documents I create or place on the District computer network or send or receive via e-mail belong to the District and may be looked at by District employees or others at any time, and that such information or documents will not be private in any way. I know that information or documents placed on the system also may be lost or damaged. I understand that if I misuse the electronic network or cause harm to the network or anyone else or their information or documents, that not only may I be subject to discipline, but my parents or guardians and I will be responsible for paying for such misuse or damage.

By signing below, I demonstrate that I understand and agree to the attached Policy and procedures.

Student Name (please print) _____

Student Signature: _____

Date: _____

Exhibit 2

Parent Authorization for Student Electronic Network Access

Submit to Building Principal.

*** Students are required to have a parent/guardian read and agree to the following:**

I have read this and accept the District's *Access to Electronic Networks* Policy and its implementing Rules and Regulations. 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 to restrict access to all controversial and inappropriate materials. I realize that my student might access objectionable material through the Internet. 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 understand that any unacceptable use of the computer network is grounds for suspending or revoking computer network privileges, and may result in discipline up to and including expulsion from school, as well as criminal or civil penalties.

I will indemnify the District and be liable for any losses, costs, damages, charges or fees, caused or incurred by my child relating to, or arising out of, my child's use of the District's electronic network or the violation of any District policy, rules, or regulations. I request that the District allow my student to access the computer network, and agree to hold harmless the Board of Education, its individual Board Members, employees, agents, and assigns, for any harm caused to my student or to me relating to, or arising out of, my student's use of the District computer network or the violation of any District policy.

I have discussed the terms of this *Authorization* and the District policy and procedures with my child. I hereby request that my child be allowed access to the District's Internet.

Student Name (*please print*)

Parent/Guardian Name (*please print*)

Parent/Guardian Signature

Date