

**RULES AND REGULATIONS IMPLEMENTING  
BOARD POLICY JB**

**APPROPRIATE USE OF TECHNOLOGY**

**I. Scope of Rules and Regulations and School District Authority**

These Rules and Regulations are promulgated pursuant to the Computer Network and Internet Safety, Access, and Use 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 rights of the District include, but are not limited to, those set forth in the Policy and these Rules and Regulations. 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.

**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 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.

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. Teachers and Other Non-Students**

To obtain network access, teachers and other non-students must submit a signed copy of the Teacher and Non-Student Authorization for Computer Network and Internet Access (Exhibit 3, the "Non-Student Authorization").

Unless a teacher's or other non-student'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 teacher's or other non-student'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 must be for 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 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, 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;
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;
4. Using the computer network for commercial, private, or personal financial gain, including gambling;
5. Deliberately accessing, creating, displaying, transmitting, or otherwise possessing or disseminating material which contains pornography, obscenity, or sexually explicit, pervasively lewd and vulgar, or indecent or inappropriate language, text, sounds, or visual depictions;
6. Creating or forwarding chain letters, "spam," or other unsolicited or unwanted messages;
7. 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;

8. 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;
9. Using or accessing another user's computer network account or password, with or without consent from that user;
10. 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;
11. 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.);
12. 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;
13. Participating in, or subscribing to non school-related mailing lists, newsgroups, chat services, electronic bulletin boards, or any other 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;
14. 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;
15. Any student use of the Internet which is not stated as an intended use on the Internet Use Form submitted by the student (see Section IV.B below); and
16. Attempting to commit any action which would constitute an unacceptable use if accomplished successfully.

#### **IV. Student Use of the Internet**

##### **A. Internet Safety**

The District's primary concern in maintaining Internet access is that student safety and security 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. Users must scan all such files with virus detection software before installing, executing, or copying such files onto a District computer.

**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.

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 other terms or conditions of computer network access promulgated by the Superintendent or Building Principals; 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.

**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. 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 users in order to ensure compliance with the Policy, these Rules and Regulations, other rules, regulations or other terms or conditions of computer network access promulgated 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 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. 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 security policy 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 Building Principals.

**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 may 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.

**XIII. Policy Modifications**

The Board of Education 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 of 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.



