EXHIBIT B

IRVING INDEPENDENT SCHOOL DISTRICT
STUDENT GUIDELINES FOR ACCEPTABLE USE OF TECHNOLOGY RESOURCES

These guidelines are provided here so that students and parents are aware of the responsibilities students accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMs, digitized information, communication technologies, and Internet access. In general, this requires efficient, ethical, and legal utilization of all technology resources.

1. Expectations are as follows:

    a. Student use of computers, other technology hardware, software, and computer networks, including the Internet, is only allowed when supervised or granted permission by a staff member.

    b. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center of each campus as well as posted on the District's Web site.

    c. Although the District has an Internet safety plan in place, students are expected to notify a staff member whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

    d. Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.

2. Unacceptable conduct includes, but is not limited to the following:

    a. Using the network for illegal activities, including copyright, license, or contract violations or downloading inappropriate materials, viruses, and/or software, hacking, and host file-sharing software.

    b. Using the network for financial or commercial gain, advertising, proselytizing, or political lobbying.

    c. Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.

    d. Vandalizing and/or tampering with equipment, programs, files, software, system performance, or other components of the network. Use or possession of hacking software is strictly prohibited.

    e. Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.

    f. Wasting finite resources, i.e., downloading movies or music for non-educational purposes.

    g. Gaining unauthorized access anywhere on the network.

h.   Revealing personal information, including but not limited to, the home address or phone number of one's self or another person.

i.   Invading the privacy of other individuals.

j.   Using another user's account, password, or ID card or allowing another user to access your account, password, or ID.

k.   Coaching, helping, observing, or joining any unauthorized activity on the network.

l.   Posting anonymous messages or unlawful information on the system.

m.   Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, demeaning, stalking, or slanderous.

n.   Falsifying permission, authorization, or identification documents.

o.   Obtaining copies of or modifying files, data, or passwords belonging to other users on the network.

p.   Knowingly placing a computer virus on a computer or network.

3.   Acceptable use guidelines for the District's network computer online services are as follows:

a.   General Guidelines:

(1)   Students will have access to all available forms of electronic media and communication that is in support of education and research, and in support of the educational goals and objectives of the District.

(2)   Students are responsible for their ethical and educational use of the computer online services in the District.

(3)   All policies and restrictions of the District's computer online services must be followed.

(4)   Access to the District's computer online services is a privilege and not a right. Each employee, student, and/or parent will be required to sign the Acceptable Use Policy Agreement Sheet and adhere to the Acceptable Use Guidelines in order to be granted access to District computer online services.

(5)   The use of any District computer online services in the District must be in support of education and research and in support of the educational goals and objectives of the District.

(6)   When placing, removing, or restricting access to specific databases or other District computer online services, school officials will apply the same criteria of educational suitability used for other education resources.

(7) Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to confidential information, copyrighted material, threatening or obscene material, and computer viruses.

(8) Any attempt to alter data, the configuration of a computer, or the files of another user without the consent of the individual, campus administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the District's Student Code of Conduct booklet.

(9) Any parent wishing to restrict his or her children's access to any District computer online services will provide this restriction request in writing to the principal. Parents will assume responsibility for imposing restrictions only on their own children.

b. Network Etiquette:

(1) Be polite.

(2) Use appropriate language.

(3) Do not reveal personally identifiable information or data (home address, phone number, phone numbers of other people) or contact unknown individuals.

(4) Remember that the other users of the District's computer online services and other networks are human beings whose culture, language, and humor have different points of reference from your own.

(5) Users should be polite when forwarding e-mail. The intent of forwarding e-mail should be on a need-to-know basis.

c. E-Mail:

(1) E-mail should be used primarily for educational or administrative purposes.

(2) E-mail transmissions, stored data, transmitted data, or any other use of the District's computer online services by students, employees, or any other user shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.

(3) All e-mail and all e-mail contents are property of the District.

4. Consequences are as follows:

a. The student in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use.

b. Noncompliance with the guidelines published here, in the Student Code of Conduct, and in Board policy CQ may result in suspension or termination of technology privileges and disciplinary actions. Use or possession of hacking software is strictly prohibited and violators will be subject to Phase III consequences of the Student

Code of Conduct. Violations of applicable state and federal law, including the Texas Penal Code, Computer Crimes, Chapter 33 will result in criminal prosecution, as well as disciplinary actions by the District.

c.   Electronic mail, network usage, and all stored files will not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use.

d.   The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications are governed by the Texas Open Records Act; therefore, proper authorities will be given access to their content.

IRVING ISD ACCEPTABLE USE AGREEMENT

Student Section

Student Name (print)_____Grade_____

School_____

I have read the Student Acceptable Use Guidelines. I agree to follow the rules contained in this policy. If I violate the rules, I may lose my access privilege to the District's computer on-line services and may face disciplinary action.

_____   _____
Student signature   Date

Parent section

I have read the Student Acceptable Use Guidelines. I understand that the Internet is a world-wide group of hundreds of thousands of computer networks. I agree that the Irving Independent School District does not control the content of these Internet networks. I understand that if my child violates the Acceptable Use Guidelines, his or her access privilege to the District's computer online services may be revoked and may be subject to disciplinary action. The Irving Independent School District has my permission to give network and Internet access to my child. I understand that my child will maintain this privilege as long as procedures described in the District's Acceptable Use Guidelines are followed.

I also grant permission for examples of my child's schoolwork to be published on the World Wide Web as an extension of classroom studies, provided that the home address, home phone number, student's last name, or a close-up photograph is not included.

Note: While the District will use filtering technology to restrict objectionable material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use. Parents who do not want their child to have Internet access and/or have their schoolwork published on the Web should submit this request in writing annually to their child's principal. While the District will attempt to restrict access, it is ultimately the responsibility of the parent to ensure his or her child does not violate this request.

_____   _____
Parent or Guardian signature   Date

_____
Parent name (print)

_____   _____
Home address   Phone