MINEOLA UFSD ACCEPTABLE USE CONTRACT

Student Name: _____ Grade: _____

School: _____ Year of High School Graduation: _____

I understand that my use of the Internet, Wide Area Network and/or e-mail provided by the Mineola School District should be restricted to areas that have educational value and related to class work and/ or approved self-discovery activities.

I have read the District's Acceptable Use Policy and Regulation and Internet Safety Policy and Regulation. I understand and agree to follow these rules. I understand that if I violate the rules, my account can be suspended or cancelled and I may face other disciplinary actions, up to and including expulsion, and/or appropriate legal action.

- I will not give out personal information such as my home address, telephone number, or the name and location of my school without my teacher's permission.
- I will be polite at all times and use appropriate language.
- I will not answer any message that is hateful or in any way makes me feel uncomfortable. If I receive a message like that, I will tell my teacher or the person in charge right away.
- I will not send any pictures or anything else without checking with my teacher.
- I will treat people on-line the way I would want them to treat me, with respect.
- I will not use the Internet Wide Area Network or e-mail for commercial purposes and/or gain to access any inappropriate sites or to engage in or support any illegal or inappropriate activity.
- I will not make any attempt to breach the security of the district's Wide Area Network.

You must sign and return the Acceptable Use Contract indicating that you are fully aware of and agree to the terms and conditions of the policy and regulation to be able to use the Wide Area Network, Internet and/or e-mail in school. This document must be signed before this student will be allowed access to the Wide Area Network, Internet and/or e-mail.

I have read, understand and agree to comply with the terms of this Acceptable Use Contract.

_____ _____

Student's Signature Date

Parent/Guardian: My child and I have read the Acceptable Use Contract and Regulation. I understand that this access is designed for educational purposes. I also recognize that while protective measures, including filtering software, have been put in place, it is impossible for the Mineola UFSD and its employees to guarantee that complete access to controversial materials via the Internet, the Wide Area Network and/or e-mail will be precluded. I will not hold them responsible for my child, should he or she access such materials on the Internet or via e-mail. Further, I am aware that there are commercial services available on the Internet and via e-mail, and any charges incurred by me or my child regarding such services will be my responsibility and not the District's. I also release the District from any and all claims of damages of any nature arising from my or my child's use or inability to use the system.

_____ _____

Parent's Signature Date

Please sign and return one copy to your child's school.

Date Adopted 9/12/02 (Revised 4/20/04)

ACCEPTABLE USE POLICY

OVERVIEW

The Mineola Union Free School District is pleased to offer students and staff access to the district's technology resources including electronic mail, data storage and the Internet for educational purposes. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation and communication. This policy will be distributed to all students and staff annually.

Our school community will find these tools a powerful means of providing access to libraries, current events, and many other useful forms of information from around the world. However, there are concerns about users accessing inappropriate materials and/or inappropriate use of the technology.

In an attempt to prevent inappropriate use of the district's technology resources, the following precautions have been taken in your child's school:

- Students and their work are supervised while using the Wide Area Network which includes the Internet. All students and parents are required to sign the attached agreement before students are allowed to utilize the district's technology resources.
- All computers with Internet capability will have a filter with the purpose of blocking access to inappropriate sites.
- Access to e-mail privileges will be granted when it is determined that it is educationally appropriate.
- Violation of the Acceptable Use Policy may result in forfeiture of the privilege of access to and use of the district's technology resources and may also result in disciplinary and/or appropriate legal action, subject to the discretion of the Superintendent of Schools or at the discretion of the Building Principal.

In addition, the Board of Education has adopted an Internet Safety Policy and Regulation in compliance with the Children's Internet Protection Act. (See policy attached)

REGULATIONS

1. TERMS AND CONDITIONS

Students/staff ("users") agree to seek information that has educational value in the context of the Mineola Public School setting. This means that the users are seeking information directly related to class work and/or approved self-discovery activities.

2. PRIVILEGES

The use of the technology is a privilege, not a right. Inappropriate use may, in the district's discretion, result in a cancellation of privileges, as well as appropriate disciplinary action. The school or district may prohibit the use of its technology resources.

3. ACCEPTABLE USES

The Mineola School District provides students/staff with network Internet and/or e-mail access to support research and education, by providing access to unique resources and the opportunity for collaborative work. The use of school access must be in support of education.

4. UNACCEPTABLE USES

Violation of any school, state or local rule, law or regulation is prohibited. This includes, but is not limited to:

- Plagiarism and copyright infringement
- Threatening or obscene material
- Expressions of bigotry, racism or hate
- Transmission of material protected by trade secret
- Unauthorized entry into the district's Wide Area Network or any attempt thereof, including but not limited to any data files and/or e-mail to which the user does not have ownership or access privileges.
- Any other illegal or inappropriate activity.

In addition, school policy prohibits:

- Commercial, religious or political activities, except in the context of officially sanctioned school activities.

5. NETIQUETTE

All users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:

- Be polite at all times.
- Use appropriate language.
- Safeguard personal information. Do not reveal a personal address, phone number, or credit card number to anyone else.
- Do not use e-mail without the permission of the teacher in charge. There should be no expectation of privacy when using the District's e-mail system, as the School District and its administration retain access to all e-mail. People who operate the system do have access to all mail. Messages relating to or in support of illegal or inappropriate activities may be reported to the authorities.
- All users of the e-mail system should also be aware that they face potential discipline for failing to abide by the terms of the Acceptable Use Policy and for the content of any e-mail which violates the policy.

6. MONITORING

All communication and information accessible via technology resources are regarded as school property. This applies to any information generated and/or distributed over the district's Wide Area Network as well. Users should not expect that e-mails or files stored on the district's storage areas would be guaranteed privacy. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Messages relating to or in support of illegal or irresponsible activities may be reported to the authorities.

7. WARRANTIES

The District **DOES NOT** provide warranties of any kind, whether expressed or implied, for the service it is providing. The Board and the District will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by the District's negligence or by the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The Board and District specifically deny any responsibility.

8. SECURITY ISSUES

Security on any computer system is a high priority, especially when the system involves many users. If a security problem on the Internet arises, notify the teacher in charge. Attempts to log on to the Wide Area Network in the name of another individual will result in cancellation of user privileges and/or disciplinary and/or appropriate legal action. Any user, attempting to breach security or having a history of causing problems with other computer systems, may be denied access to the Wide Area Network.

.

9. VANDALISM AND HARASSMENT

Vandalism and harassment will result in **CANCELLATION OF PRIVILEGES AND/OR DISCIPLINARY AND/OR LEGAL ACTION**. Vandalism is defined as any malicious attempt to harm or destroy data or hardware, or to change the operating configuration of any computer or any networks connected to the computer. This includes, but is not limited to, the uploading or creation of computer viruses or attempts to modify the operating system. Harassment is defined as the persistent annoyance of another user. Harassment includes, but is not limited to, the circulation and/or sending of unwanted, inappropriate, obscene or threatening messages.

INTERNET SAFETY POLICY

The Board of Education is committed to undertaking efforts that serve to make safe for children the use of district computers for access to the Internet and World Wide Web. To this end, although unable to guarantee that any selected filtering and blocking technology will work perfectly, the Board directs the Superintendent of Schools to procure and implement the use of technology protection measures that block or filter Internet access by:

- adults to visual depictions that are obscene or child pornography, and
- minors to visual depictions that are obscene, child pornography, or harmful to minors, as defined in the Children's Internet Protection Act.

Subject to staff supervision, however, any such measures may be disabled or relaxed for adults conducting bona fide research or other lawful purposes, in accordance with criteria established by the Superintendent or his or her designee.

To the extent practical, the Superintendent or his or her designee also shall develop and implement procedures that provide for the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of students using district computers; and restricting student access to materials that are harmful to minors.

In addition, the Board prohibits the unauthorized disclosure, use and dissemination of personal information regarding students; unauthorized online access by students, including hacking and other unlawful activities; and access by students to inappropriate matter on the Internet and World Wide Web. The Superintendent or his or her designee shall establish and implement procedures that enforce these restrictions.

The computer network coordinator, designated under the district's Computer Network or Acceptable Use Policy, shall monitor and examine all district computer network activities to ensure compliance with this policy and accompanying regulation. He or she also shall be responsible for ensuring that staff and students receive training on their requirements.

All users of the district's computer network, including access to the Internet and World Wide Web, must understand that use is a privilege, not a right, and that any such use entails responsibility. They must comply with the requirements of this policy and accompanying regulation, in addition to generally accepted rules of network etiquette, and the district's Acceptable Use Policy. Failure to comply may result in disciplinary action including, but not limited to, and revocation of computer access privileges.

Ref: Public Law No. 106-554
47 USC § 254
20 USC § 6801

Date Adopted 9/12/02 (Revised 4/20/04)

INTERNET SAFETY POLICY REGULATION

The following rules and regulations implement the Internet Safety Policy adopted by the Board of Education to make safe for children the use of district computers for access to the Internet and World Wide Web.

I. Definitions

In accordance with the Children's Internet Protection Act,

- *Child pornography* refers to any visual depiction, including any photograph, film, video, picture or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. It also includes any such visual depiction that (a) is, or appears to be, of a minor engaging in sexually explicit conduct; or (b) has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or (c) is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.
- *Harmful to minors* means any picture, image, graphic image file, or other visual depiction that (a) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (b) depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (c) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

II. Blocking and Filtering Measures

- The Superintendent or his or her designee shall secure information about, and ensure the purchase or provision of, a technology protection measure that blocks access from all district computers to visual depictions on the Internet and World Wide Web that are obscene, child pornography or harmful to minors.
- The district's computer network coordinator shall be responsible for ensuring the installation and proper use of any Internet blocking and filtering technology protection measure obtained by the district.
- The computer network coordinator or his or her designee may disable or relax the district's Internet blocking and filtering technology measure only for adult staff members conducting research related to the discharge of their official responsibilities and for students for approved educational purposes.
- The computer network coordinator shall monitor the online activities of adult staff members for whom the blocking and filtering technology measure has been disabled or relaxed to ensure there is not access to visual depictions that are obscene or child pornography.

III. Monitoring of Online Activities

- The district's computer network coordinator shall be responsible for monitoring to ensure that the online activities of staff and students are consistent with the district's Internet Safety Policy and this regulation. He or she may inspect, copy, review, and store at any time, and without prior notice, any and all usage of the district's computer network for accessing the Internet and World Wide Web and direct electronic communications, as well as any and all information transmitted or received during such use. All users of the district's computer network shall have no expectation of privacy regarding any such materials.

- Except as otherwise authorized under the district's Computer Network or Acceptable Use Policy, students may use the district's computer network to access the Internet and World Wide Web only during supervised class time, study periods or at the school library, and exclusively for research related to their course work.
- Staff supervising students using district computers shall help to monitor student online activities to ensure students access the Internet and World Wide Web, and/or participate in authorized forms of direct electronic communications in accordance with the district's Internet Safety Policy and this regulation.
- The district's computer network coordinator shall monitor student online activities to ensure students are not engaging in hacking (gaining or attempting to gain unauthorized access to other computers or computer systems), and other unlawful activities.

IV. Training

- The district's computer network coordinator shall provide training to staff and students on the requirements of the Internet Safety Policy and this regulation at the beginning of each school year.
- The training of staff and students shall highlight the various activities prohibited by the Internet Safety Policy, and the responsibility of staff to monitor student online activities to ensure compliance therewith.
- Student shall be directed to consult with their classroom teacher if they are unsure whether their contemplated activities when accessing the Internet or World Wide Web are directly related to their course work.
- Staff and students will be advised to not disclose, use and disseminate personal information about students when accessing the Internet or engaging in authorized forms of direct electronic communications.
- Staff and students will also be informed of the range of possible consequences attendant to a violation of the Internet Safety Policy and this regulation.

V. Reporting of Violations

- Violation of the Internet Safety Policy and this regulation by students and staff shall be reported to the Building Principal.
- The Principal shall take appropriate corrective action in accordance with authorized disciplinary procedures.
- Penalties may include, but are not limited to, the revocation of computer access privileges, as well as school suspension in the case of students and disciplinary charges in the case of teachers.