WATCHUNG HILLS
REGIONAL HIGH SCHOOL

Elizabeth C. Jewett
Superintendent

Timothy M. Stys, CPA
Business Administrator

George P. Alexis
Principal

Student Permission for Internet Access

Each student and his/her parent/guardian must sign the Student Permission form before the student is granted access to a live Internet connection and use of the school network. Please read this document carefully before signing.

All use of the Internet will be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. The Internet is a fluid environment, the information which may be available to users is constantly changing; therefore, it is the users responsibility to limit their access to material used for educational purposes only. **The failure of any user to follow the terms of the *Permission for Internet Access* will result in the loss of Internet privileges, disciplinary action, and/or appropriate legal action.** The signature at the end of this document is legally binding and in dictates that the signatories have read the terms and conditions carefully and understand their significance.

Terms and Conditions

1. Acceptable Use – All use of the District' s connection to the Internet must be in support of education and/or research , consistent with the educational objectives policies, rules, and regulations of the Board of Education, and in compliance with and subject to District and building discipline codes.

2. Privileges – The use of the District's Internet is a privilege, not a right. Therefore, inappropriate use will result in a cancellation of those privileges. The system administrator will make all decisions regarding whet her a user has violated the *Permission* and may deny, revoke, or suspend access at any time. **Violations of the *Permission* may result in the loss of Internet privileges and student discipline. Due process will be to commensurate with the seriousness of the offense.**

3. Internet Safety – The District will take appropriate measures to ensure:

   a. That minors are not provided with access to inappropriate matter on the Internet and World Wide Web. Determinations regarding what matter is inappropriate for minors (individuals under the age of 17) will be made by the Board, using criteria it deems appropriate;
   b. The safety and security of minors when using electronic mail chat rooms, and other forms of direct electronic communications;
   c. That minors are prevented from gaining unauthorized access including so-called hacking, and other unlawful activities, while online;
   d. That there is no unauthorized disclosure, use or dissemination of personal identification information regarding minors;

4. Unacceptable Use – The user is responsible for his/her actions and activities involving the network. Some examples of unacceptable uses are given below. However, the list is not intended to be complete. The Administration may periodically revise the concepts to acceptable and unacceptable use. Thereupon, these revisions will become part of this document.

   a. Using the network for any illegal activity, including the violation of copyright or other contracts, or transmitting any material in violation of any federal or State regulations. This includes but is not limited to music, games, and movies;

   b. Unauthorized access or downloading of software, electronic files, e-mail, or other data (commonly referred to as "hacking");
   c. Downloading copyrighted material for other than legal personal or professional use;

   d. Invading the privacy of individuals;

   e. Using another user's account or password;

   f. Posting material authored or created by another without his/her consent;

   g. Using the network for commercial or private advertising;

   h. Accessing, submitting, posting, publishing, or dis playing any defamatory, knowingly inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material;

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

   j. Publishing or otherwise disseminating another person's identity, personal information, account, or password;

   k. Using the network for unauthorized product advertisement, political activity, promoting or encouraging the use of illegal or controlled substances;

   l. Forgery or alteration of e-mail;

   m. Unauthorized use of the network to play computer games, enroll in list serves;

   n. Having food or beverages near the computers;

   o. Using peer to peer file sharing services i.e. Kazaa or Napster;

   p. Attempting to change security settings or spread computer viruses and/or worms;

   q. Installing software or making unauthorized changes to computer settings.

   The first time these rules are broken, the user' s account privileges will be revoked for two weeks. Further violations will be dealt with by the administration on an individual level.

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

   a. Be polite. Do not become abusive in your messages to others.

b. Use appropriate language. Do not swear, or use vulgarities or any ot her prohibited language.
c. Do not reveal the personal addresses or telephone numbers of students or staff.
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.

6. 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 suffered by users. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or user errors or omissions. The use of any information obtained through Internet services.

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 no demonstrate the problem to other users. Keep y our account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the network as a system administrator will result in cancellation of users' 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 the networks, software, hardware, an d data of the District, another user the Internet, or any other network. This term/condition prohibits degrading or disrupting equipment, software, or system performance. It also includes, but is not limited to, the uploading or creation of computer viruses. Users are responsible for any and all costs related to the repair or rest oration of any damage done through vandalism. The District will use the legal system to seek restitution.

We understand that Internet access is designed for educational purposes. But, even though the District provides and operates a technology protection measure (filtering), with respect to any of its computers with Internet access, we recognize that it is impossible for the District to restrict access to all controversial and inappropriate materials and/or web sites. Therefore, we hereby release the School District and its Boar d members, employees, and agents from any claims and damages arising from my child's use of, or inability to use the Internet. We understand that the District is not responsible for any unauthorized costs or charges incurred by the student nor will the District be responsible for the accuracy of information obtained from the Internet. We accept full responsibility for supervision if and when the child's use is not in a school setting. We understand that should my child commit any violation, the child's access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. The undersigned have discussed the terms of this Authorization. We hereby request that the student be allowed access to the District's Internet.

By electronically signing this document, I acknowledge that I have read and understand this information and agree with its terms.

This agreement will remain in effect for the entire time the student is actively enrolled in Watchung Hills Regional High School.