PISCATAWAY BOARD OF EDUCATION
Technology / Internet Access Agreement

ACCEPTABLE USE POLICY

The Piscataway Board of Education's Acceptable Use Policy ("AUP") is in place to prevent unauthorized access and other unlawful activities by users online; prevent unauthorized disclosure of or access to sensitive information; and to comply with the Children's Internet Protection Act ("CIPA"). As used in this policy, "user" includes anyone using the computers, Internet, email, chat rooms, instant messaging (IM), peer-to-peer (P2P), and other forms of direct electronic communications or equipment provided by the Piscataway School District's network (the "network."). It also covers any outside equipment that uses the District's network to access the Internet.

The Board of Education will use technology protection measures to block or filter, to the extent possible, access of visual depictions that are obscene, pornographic, and harmful to minors over the network. The Board of Education reserves the right to monitor users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of Piscataway School District property, network and/or Internet access or files, including email.

Schools must qualify students using the computer network and Internet access at the beginning of each school year with a signed agreement to this AUP. Students who are under 18 must have their parents or guardians sign the AUP agreement and schools must keep the signed page on file. Once signed, the permission/acknowledgement page remains in effect until revoked by the parent, or the student loses the privilege of using the District's network due to violation of the policy or is no longer a student of this District. A copy of the signed agreement form and the sample letter to parents/guardians are contained in the regulations supporting this policy.

The Board of Education recognizes the importance of student safety in the use of Internet access. Information on safe practices is reinforced with students at all times, including but not limited to:

1. Students under the age of eighteen should only access District accounts outside of school if a parent or legal guardian supervises their usage at all times. The student's parent or guardian is responsible for monitoring the minor's use;

2. Students shall not reveal on the Internet personal information about themselves or other persons. For example, students should not reveal their name, home address, telephone number, or display photographs of themselves or others;

3. Students shall not meet in person anyone they have met only on the Internet; and

4. Students must abide by all laws, this Acceptable Use Policy and all District security policies.

The Board of Education reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for the District, students, employees, schools, network or computer

PISCATAWAY BOARD OF EDUCATION
Technology / Internet Access Agreement

ACCEPTABLE USE POLICY (Continued)

resources, or (2) that expend District resources on content the District in its sole discretion determines lacks legitimate educational content/purpose, or (3) other activities as determined by District as inappropriate. The following are some examples of inappropriate activity in the use of the District's equipment and/or access to the world-wide web:

- Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials;

- Criminal activities that can be punished under law;

- Selling or purchasing illegal items or substances;
- Obtaining and/or using anonymous email sites; spamming; spreading viruses;

- Causing harm to others or damage to their property, such as:

  1. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
  2. Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
  3. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or down loading computer viruses or other harmful files or programs, or disrupting any computer system performance;
  4. Using any District computer to pursue "hacking," internal or external to the District, or attempting to access information protected by privacy laws; or
  5. Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes".

- Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:

  1. Using another's account password(s) or identifier(s);
  2. Interfering with other users' ability to access their account(s); or
  3. Disclosing anyone's password to others or allowing them to use another's account(s).

- Using the network or Internet for Commercial purposes:

  1. Using the Internet for personal financial gain;
  2. Using the Internet for personal advertising, promotion, or financial gain; or

PISCATAWAY BOARD OF EDUCATION
Technology / Internet Access Agreement

ACCEPTABLE USE POLICY (Continued)

3. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes.

The Board of Education also provides some students with electronic communications tools including instant messaging (IM), blogging, responding in discussion boards, wikis and other tools deemed educationally appropriate. This Acceptable Use Policy ("AUP") governs usage and content standards for IM and applies to all messages on the School District networks and systems at District and School sites, as well as at remote locations, including but not limited to students', homes or other locations.

- School District users are prohibited from downloading and using personal, consumer-grade IM software (AOL Instant Messenger, Yahoo, MSN) to transmit IM via the public Internet. Students who violate this rule are subject to disciplinary action.

- All communications and information transmitted, received, or archived in the School District system belong to the District.

- Users have no reasonable expectation of privacy when using the District's computing system. The Board of Education reserves the right to monitor, access, and disclose all electronic communication.

- Messages must be treated as legitimate records that may be retained and used as evidence in litigation and investigations.

- Users should refrain from causing harm to others and assure that language used in electronic communications is appropriate and non-offensive. The District policy specifically prohibits using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, or transmitting offensive, harassing, or disparaging materials;

- Students should refrain from sending jokes, rumors, or gossip. These communications, which often contain objectionable material, are easily misconstrued when communicated electronically.

- District electronic communication systems are for educational use only.

The Board of Education holds that the use of a District account is a privilege, not a right, and misuse will result in the restriction or cancellation of the account. Misuse may also lead to disciplinary and/or legal action for students including suspension, expulsion, or criminal prosecution by government authorities. The Board of Education will attempt to tailor any disciplinary action to the specific issues related to each violation.

The Board of Education makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the District's network are to be borne by the user. The Board of Education also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the Piscataway Board of Education, its affiliates, or employees.

PISCATAWAY BOARD OF EDUCATION

Internet Tips for Parents

- Become more computer literate so you can learn how to block objectionable material.
- Keep the computer in a common area in your home, where you can watch and monitor your child.
- If you allow your child to have access to email, monitor your child's email by sharing an email account.
- Make your child's favorite sites easy to find by bookmarking them
- Take time to go online with your child so he or she can develop healthy online behavior.
- Block dangerous or threatening sites, such as private chat rooms, with safety features provided by your ISP (Internet Service Provider) or install a filtering program.
- Be aware and inform your child that anything posted on the Internet is there forever. Also, anytime they post something on a blog, they are revealing their email address.
- Be on the lookout for any unfamiliar charges to your credit card and/or phone bills, which could indicate online activity involving your child
- Be sure you are aware of any Internet access your child has away from home. Find out if safety features are in place at your child's school, after-school center, friends' homes, or any place where he or she could use a computer without your supervision.
- Don't ever dismiss your child's concerns while online. If your child reports feeling uncomfortable about an online exchange, take him or her seriously.
- Alert the appropriate authorities immediately should you or your child receive copies of any obscene or threatening messages.
- Call the National Center for Missing and Exploited Children at (800) 843-5678 if you are aware of the transmission, use, or viewing of child pornography online. Contact your local law enforcement agency or the FBI if your child has received child pornography via the Internet.
- Many sites use "cookies," devices that track specific information about the user, such as name, email address, and shopping preferences. Cookies can be disabled. Ask your Internet service provider for more information.

Rules for Your Child

- Follow the rules set by your parents, as well as those set by your Internet service provider.
- Never trade personal photographs in the mail or scanned photographs over the Internet.
- Never reveal personal information, such as address, phone number, or school name or location.
- Use screen names that do not include your real name.
- Never agree to meet anyone from a chat room in person.
- Never respond to a threatening email or message.
- Always tell a parent about any communication or conversation that was scary or made you uncomfortable.

PISCATAWAY BOARD OF EDUCATION

ACCEPTABLE USE POLICY AGREEMENT

We have read, understand, and agree to abide by the provisions of the Acceptable Use Policy of the Piscataway Township School District.

Date: School:

Student Name: Student Signature:

Parent/Legal Guardian Name: Parent/Legal Guardian Signature: