STUDENT INTERNET SAFETY AND TECHNOLOGY ACCEPTABLE USE POLICY (AUP)

Plymouth Public Schools provides Internet access for educational purposes for their students, ensuring that students develop global communication and 21st century skills.

Plymouth Public Schools filters the Internet in compliance with the Children's Internet Protection Act (CIPA). The combination of the filter, appropriate student use, and teacher supervision ensures safe access to the Internet. However, we still cannot guarantee that your child will not find material on the Internet that may be considered objectionable. Student use of the network is restricted to educational purposes only. Personal electronic devices are subject to the same restrictions.

1.0 District Responsibilities

1.1 The Coordinator of Educational Technology and Instructional Media (CETIM) will oversee access to the network and will establish processes for the following: authorization for software installation; back-up and archiving of databases; virus protection; and compliance with.

1.2 The Principal or designee will maintain signed user agreements, and be responsible for enforcing the Technology AUP.

1.3 When using the Internet for class activities, teachers will make every attempt to preview and select material appropriate to the students and relevant to the course objectives. Teachers will provide guidelines and resources to assist their students in developing the necessary critical thinking skills to access online information.

2.0 Access to the System

2.1 The Technology AUP will govern all utilization of the network. Student use of the system will also be governed by applicable sections of the Plymouth School Committee Policy Handbook and the Student Handbook.

2.2 Students will have access to the Internet through the District's networked computers. Parents/Guardians may specifically request that their children not be provided such access by checking the appropriate box on the signature page of the AUP and returning it to their child's school. Upon receipt of that form, Plymouth Public Schools will make its best effort to restrict all Internet access. However, there can be no guarantee that a student can be restricted at all times.

2.3 Students will have access to second generation and subsequent generations of the World Wide Web that allow students to collaborate and share online. Students will be educated about appropriate behavior, including cyber bullying awareness and response (See Plymouth Public Schools Anti-Bullying Policy 6.15), instant messaging, inappropriate texting and interacting with other individuals on social networking sites and in chat rooms.

2.4 Students should not use the following without authorization:

- Social Networking
- Instant Messenger
- Chat Rooms
- Personal Wireless Devices

3.0 District Limitation of Liability

Plymouth Public Schools makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through its network will be error-free or without defect. The district will not be responsible for any damages users may suffer, including but not limited to, loss of data or interruptions of service, or personal physical, psychological, or monetary damages. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The district will not be responsible for unauthorized financial obligations arising through the use of the system.

4.0 Due Process

4.1 When using the network, the user agrees to take full responsibility for his or her actions. The Plymouth Public Schools will not be held liable for the actions of anyone connecting to the Internet through this network. Therefore, all users shall assume full liability, legal, financial, or otherwise, for their use of the network.

4.2 Violations of the Technology AUP can carry serious consequences and could result in the immediate suspension of the user's privileges. Further disciplinary action may be taken by the Administration of the Plymouth Public Schools and/or Town, County, State or Federal authorities. Disciplinary actions will be tailored to meet specific concerns related to the violation. These disciplinary actions may include suspension or expulsion.

4.3 Any question or allegations concerning adherence to the Technology AUP should be brought to the attention of the CEITM.

5.0 Search and Seizure

5.1 The network is the property of the school department and its storage systems are therefore subject to inspection by the administration at any time. System users have a limited privacy expectation in the contents of their personal files on network.

5.2 An individual search will be conducted if there is suspicion that a user has violated the AUP, the law or the disciplinary code. The nature of the investigation will be in the context of the nature of the alleged violation.

6.0 Unacceptable Use

The user of the Plymouth Public Schools Internet connection and network becomes an extension of the Plymouth Public Schools and is expected to abide by the rules set forth in the Student Handbook where applicable. Inappropriate behavior will not be allowed. The user will not use computers / Internet for any purpose that is inconsistent with the educational purpose intended, such as, but not limited to:

- using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language
- engaging in personal attacks, including prejudicial or discriminatory attacks
- knowingly or recklessly posting false or defamatory information about a person or organization or posting information that could cause damage or disruption. This includes, but is not limited to, the posting of broadcast messages or other actions that cause congestion of the network or interfere with the work of others.
- installing unauthorized software or downloading unauthorized software from a remote location or joining listserves or newsgroups without express permission of instructional staff.
- attempting to go beyond his or her authorized access, making deliberate attempts to disrupt system performance or destroy data (by spreading computer viruses or by any other means), or engaging in other illegal activities.
- disseminating passwords, codes, access telephone numbers, or account numbers to unauthorized persons.
- using the network to access or send material that is profane or obscene (e.g., pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (e.g., hate literature).
- changing in any way the configuration of a computer or network without permission of instructional staff.
- damaging or vandalizing computers, computer systems or networks.
- trespassing in other’s folders, work or files or using another’s password.
- intentionally wasting resources, such as paper, ink cartridges, ribbons, storage space, diskettes, etc.
- using computers / Internet to play non-educational games or other non-academic activities.
- participating in any type of teleconferencing or chat without permission of instructional staff.
- using e-mail without instructional staff permission / supervision.

- The network may not be used for personal and commercial purposes, such as, but not limited to, offering or purchasing goods and/or services for personal use.

7.0 Safety

The safety of the Internet user is of utmost concern. Personal safety for the user means never giving out personal information such as home addresses or telephone numbers for the user or others. Users will not agree to meet with someone they have met on-line without parent/guardian approval and participation. Users will promptly disclose to their teacher or other school employees any message they receive that is inappropriate or that makes them feel uncomfortable.

8.0 Web Publishing

The Plymouth Public Schools web site is designed to provide a portal to enable communication among teachers, students, staff, administration and the community, both local and global. Material posted on the District's web site must reflect the high educational standards of the Plymouth Public Schools.

To insure the safety of our students and the accuracy and security of district information the guidelines and procedures listed below must be followed:

8.1 No student's personal information, such as SIMS (Student Information Management Systems) data, last name, home address, and telephone number may be posted on the web site. Students must submit a signed permission form from their parent/guardian granting permission to post the student's work or picture.

8.2 Requests to post material on the Plymouth Public Schools' Web site must have prior approval of the Principal or designee.

8.3 Student directory information may not be published.

8.4 The creator of a home page on the District's network is responsible for insuring that the information contained therein is of the highest editorial standards (spelling, punctuation, grammar, style, etc.). The information should be factually accurate and current. If errors are observed, the CETIM or designated school page editor should be contacted to make the necessary corrections.

* It should be noted that the Plymouth Public Schools name or logo may not be used on a personal web page without permission of the Superintendent.

9.0 Plagiarism and Copyright Infringement

Existing copyright law will govern the use of material accessed through network. The user will not plagiarize works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours. All copyrighted material used must have the express written permission of the person or organization that owns the copyright.

10.0 Student Technology AUP Access Agreement

Your signature on this document is legally binding, and indicates that you have read the terms and conditions carefully and understand their significance and consequences. This policy is further supported by the rules and regulations found in each school's student handbook and discipline policies.

		REVISION 1:		**REVISION 2:**	
Information:	October 6, 1997	Information:	April 5, 2004	Information:	May 18, 2009
Discussion:	November 17, 1997	Discussion:	April 5, 2004	Discussion:	May 18, 2009
Adopted:	November 17, 1997	Approval:	April 26, 2004	Approval:	May 18, 2009