STAFF TECHNOLOGY ACCEPTABLE USE POLICY (AUP)

Plymouth Public Schools recognizes the value of teacher inquiry, investigation, and innovation using technology tools to enhance learning. Plymouth Public Schools recognizes an obligation to teach and ensure responsible and safe use of technology by their staff.

This policy addresses staff use of the district network, email, web publishing, personal computers, and publicly available social media networks including personal web sites, blogs, wikis, social networks, online forums, virtual worlds, and any other sites considered social media. The use of professional social media is an extension of the classroom. Whether at home or in school, anything considered inappropriate in the classroom is also inappropriate in the use of social media.

1.1 Purpose

1.2 Plymouth Public Schools provides employees and students access to the Plymouth Public Schools Local and Wide Area Network (hereinafter referred to as the network), that also serves as our gateway to the Internet.

1.3 The network has been developed for educational purposes. It is intended to assist in preparing students and teachers for success in life in the 21st century by providing access to a wide range of information resources and the ability to communicate with people throughout the world. The term "educational purposes" includes use of the network for curriculum activities, research, and professional or career development activities related to education.

1.4 The network will be used to enhance productivity through increased communication within the district, with parents, social service agencies, government agencies, businesses, etc.

1.5 The network may not be used for personal and/or commercial purposes, including (but not limited to) offering or purchasing goods and/or services for personal use.

2.1 Responsibilities

2.2 The District Network Engineer and the Coordinator of Educational Technology and Instructional Media will oversee access to the network and will establish processes for: authorization for software installation; back-up and archival of databases; virus protection; and compliance with the Children's Internet Protection Act (CIPA).

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

2.4 When using the Internet for class activities, teachers will have previewed and selected material appropriate to the students and relevant to the course objectives. Teachers will aide students in developing critical thinking skills (i.e., assessing reliability of information found on the Internet) and provide guidelines and resources to assist their students in focused research activities.

3.0 District Limitation of Liability

3.1 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, network infrastructure, or district-owned or -leased devices 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 caused by any reason, 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 termination of employment.

4.3 Any question or allegations concerning adherence to the Technology Acceptable Use Policy should be brought to the attention of the Coordinator of Educational Technology.

5.0 Monitoring and Privacy

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 stored on or accessed through the network. Records of electronic device use may be subject to public records law and may be discoverable in criminal or civil proceedings.

5.2 All Plymouth Public Schools email and files, either downloaded or copied from the Plymouth Public Schools system, that are accessed through a user's home computer or any other non-Plymouth Public Schools computer or device, are Plymouth Public Schools' property and should be used and protected according to this policy and other applicable policies and laws governing information confidentiality and security.

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

5.4 Technicians and computer system administrators maintain full access rights to all storage devices, and may need to access/manage such storage devices as part of their duties.

5.5 The Plymouth Public Schools prohibits the use of camera and audio recording functions on any equipment, including but not limited to personal cameras, personal camera telephones, and/or school-issued devices, at school or school-sponsored events, except when specifically authorized by school administration or staff and with knowledge and consent of the participants. In no event should any photographs or video be taken of confidential information, nor should photographs, audio, or video recordings be made without knowledge of the subjects. Audio recording without the consent of the individuals recorded may result in criminal felony charges. M.G.L. c. 272 § 99.

6.0 Unacceptable Use

When faculty and staff of the Plymouth Public Schools use the Plymouth Public Schools network connection, Plymouth Public Schools -owned or -leased device, or any personal electronic device connected to the Plymouth Public Schools network, they become an extension of the Plymouth Public Schools and are expected to follow the guidelines of this policy. Inappropriate use in violation of this policy, the staff handbook, school committee policies, and state and federal laws or regulations will not be allowed. Access to the Internet, other electronic resources, and the hardware is a privilege, not a right, and carries with it responsibilities for safe and respectful use.

Requirements:

- Employees must be respectful and professional in all communications (by word, image, text or any other means). Employees shall not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- Employees should not engage in personal attacks, including prejudicial or discriminatory attacks or harassment of any kind; they should not knowingly or recklessly post false or defamatory information about a person or organization, or post 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.
- Employees should not install unauthorized software or download unauthorized software from a remote location without express permission of the Coordinator of Educational Technology and Instructional Media or the District Network Engineer.
- Employees should not attempt to go beyond their authorized access, make deliberate attempts to disrupt system performance or destroy data (by spreading computer viruses or by any other means), or engage in other illegal activities; they should not change in any way the configuration of a computer or network without permission of administration or technology staff.
- Employees should not disseminate passwords, codes, access telephone numbers, or account numbers to unauthorized persons.
- Employees should not use 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).
- Employees should not damage or vandalize computers, computer systems, or networks.
- Employees should not trespass in other's folders, work or files, or use another's password.
- The network may not be used for personal and commercial purposes, including, but not limited to, offering or purchasing goods and/or services for personal use.
- Employees may not engage in electronic forgery, credit card fraud, or other illegal behavior.

7.0 E-Mail

7.1 All e-mail created or received by an employee of a governmental unit is a public record. According to Massachusetts General Laws, the term "public record" is defined as all documentary materials or data created or received by any officer or employee of a governmental unit, regardless of physical form or characteristics. G. L. c. 4 S 7(26). E-mail is, therefore, a public record and it is subject to the requirements of the Public Records law, G.L. c. 66. Any member of the public may request copies of e-mail. Please note that even deleted messages are subject to disclosure because they still exist on backup drives.

7.2 Users should consider e-mail messages equivalent to letters sent on official letterhead and therefore should be written in a professional and courteous tone.

7.3 Faculty and staff must not subscribe to mass electronic mailings (e.g., chain letters, Joke of the Day, Horoscopes, Trivia, etc.). Mass mailings take up valuable network space that should be used for educational purposes.

7.4 The Coordinator of Educational Technology and Instructional Media or the Systems Engineer monitors the network to ensure proper network operations. Principals, Department Heads or Supervisors may request detailed reports indicating e-mail and Internet usage.

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. Material posted on the district's web site or web portal must reflect the high educational standards of the Plymouth Public Schools.

To ensure 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 have signed permission from their parent/guardian granting permission to post the student's work.

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

8.3 Photographs and images used must have the written permission of not only the person or organization that owns the image, but of any person or persons included within the image.

8.4 Logos or Trademarks used must have written permission from the person or organization that owns the trademark.

8.5 Student directory information may not be published.

8.6 The creator of the home page is responsible for ensuring 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 District Technology Coordinator or designated school Webmaster should be contacted to make the necessary corrections.

8.7 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 Personal Computers

9.1 Faculty and staff personal computers may be configured for Plymouth Public Schools' network with approval from the Coordinator of Educational Technology and Instructional Media or Systems Engineer.

9.2 Personal computers are not the property of Plymouth Public Schools and will not be serviced by the Technology Department.

9.3 Personal computers must have up-to-date virus protection software in order to be placed on the district's network.

9.4 Use of personal electronic devices (laptops, cell phones, etc.) connected to the Plymouth Public Schools' network must abide by this Acceptable Use Policy.

10.0 Plagiarism and Copyright Infringement

10.1 Existing copyright law will govern the use of material accessed through the 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 on the district's web page must have the express written permission of the person or organization that owns the copyright. Plymouth Public Schools will cooperate with copyright protection agencies investigating copyright infringement by users of the computer systems and network of the Plymouth Public Schools.

11.0 Modification of this Policy

The Plymouth Public Schools School Committee reserves the right to modify or change this policy and related implementation procedures at any time.

12.0 Staff 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 the Plymouth Public Schools employee handbook and discipline policies.

Review:		**Review:**		**Review:**	
Information:	July 11, 2016	Information:	Nov. 2, 2020	Information:	
Discussion:	July 11, 2016	Discussion:	Nov. 2, 2020	Discussion:	
Adopted:	July 11, 2016	Approved:	Nov. 2, 2020	Approved:	