Parent Handbook 2016-2017
Plymouth River Elementary
Pages 26-29

TECHNOLOGY DEPARTMENT

Our mission is to teach students in grades K-5 the technology curriculum according to the Massachusetts Technology Literacy Standards. These include: Standard 1: Proficiency in productivity tools such as word processing, spreadsheet, presentation, research and databases. Standard 2: Digital Citizenship which includes responsible use of technology, ethics and online safety. Standard 3: Application of technology for higher order thinking skills such as critical thinking, problem solving, decision making, collaboration, and innovation.
Our school currently houses SMARTboards in every classroom; provides access to mobile carts that include laptops, chromebooks and iPads; a computer lab; document cameras, scanners, and printers. We provide training and support to teachers in innovative technologies to help them maximize student learning in the classroom.

INTERNET/COMPUTER USE

The Hingham Public School system provides computers and technical equipment for the professional use of staff, and as educational aids for students. Use of any of the Hingham Public School District's computer systems is limited to school-related activities. Administration and classroom systems can be re-allocated at the discretion of the school administration or technology department without advance notice.

The Hingham Public School District makes no warranties of any kind, whether expressed or implied, for the computer services it is providing. Hingham Public Schools will not be responsible for any damages resulting from delays or service interruptions caused by its own negligence or your errors or omissions. Use of any information obtained via the Internet is at your own risk. Hingham Public Schools specifically denies any responsibility for the accuracy or quality of information obtained through its computer services.

The following set of technology policies applies to all users of Hingham Public Schools' computer systems. Failure to comply with the guidelines herein may result in termination, suspension, or other limitation of an employee's or student's computer privileges. These regulations may be amended and updated at the discretion of Hingham Public Schools' administration.

1. Computers, including software and hardware, are the property of Hingham Public Schools. Computer systems are to be used for school-related activities, and are not to be removed from the premises without written permission from the District Technology Manager.

2. Users should not have any expectation of privacy with respect to personal data stored on Hingham Public Schools' computers. Electronic mail (E-mail) messages are considered public records and are therefore legally discoverable and subject to record retention. Users should not expect that electronic mail messages (even those marked "Personal") are private or confidential.

3. The Hingham Public School system may monitor electronic mail and Internet activities on the schools' computer systems for reasons including, but not limited to, the following:

   a. system checks.

   b. reviews of productivity.

   c. investigations into claims of possible criminal activity.

d. investigations into inappropriate use of the District's Internet connection.

4. Use of the District's computer systems constitutes consent to monitoring of E-mail transmissions and other on-line services, and is conditioned upon strict adherence to this policy.

5. The following activities are strictly prohibited:

a) Any illegal activity, including, but not limited to, the transmission of copyright or trade secret material, or the participation in any type of criminal activity.

b) Attempts to violate the computer security systems implemented by the Hingham Public Schools, Town of Hingham, or other institutions, organizations, companies or individuals.

c) Accessing material that is inappropriate for school use, such as Internet sites promoting pornography, gambling, or hate.

d) Attempts to circumvent the Internet filtering capabilities of the Hingham Public Schools or the school systems' Internet provider(s).

e) Reproduction of copyrighted material without explicit permission.

f) The use of profanity or inappropriate language in electronic mail.

g) Use of school computer systems for political or commercial purposes.

h) Using school computer systems to send unsolicited bulk E-mail (SPAM).

i) Developing or disseminating malicious software programs, such as computer viruses.

j) Downloading, installing, or copying any commercial software, shareware, or freeware onto network drives or disks without written permission from the network administrator or District Technology Manager.

k) Misrepresentation of your identity by using another user's account, or by masking your own identity.

l) Accessing files or e-mail of another without proper authority or consent.

6. No profane, abusive, or impolite language should be used to communicate, nor should materials be accessed which are not in line with the rules of school behavior. Should a user encounter such material by accident, they should report it to an appropriate authority immediately.

7. In compliance with the Children's Internet Protection Act (CIPA), Hingham has installed filtering and/or blocking software to restrict access to Internet sites containing material harmful to minors. The software scans for objectionable words or concepts, as determined by the Hingham School District. However, no software is foolproof. A user who accidentally connects to an inappropriate site must immediately disconnect from the site and notify a teacher or supervisor. If a user sees another user accessing inappropriate sites, he or she should notify a teacher or supervisor immediately. Students and staff may not disable the District's filtering software at any time when students are using the Internet system if such disabling will cease to protect students against access to inappropriate materials. Authorized staff may temporarily or permanently unblock access to sites containing appropriate materials if the filtering software has inappropriately blocked access to such sites.

8. Staff must supervise student use of the District's Internet system in a manner that is appropriate to the students' age and the circumstances of use.

9. The following restrictions against inappropriate speech and messages apply to all speech communicated and accessed through the District Internet system, including all email, instant messages, Web pages, and Web logs:

a) Students shall not send obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful messages.

b) Students shall not post information that could cause damage, danger, or disruption, or engage in personal attacks, including prejudicial or discriminatory attacks.

c) Students shall not harass other persons, or knowingly or recklessly post false or defamatory information about a person or organization.

10. Students' home and personal internet use can have an impact on the school and on other students. If students' personal Internet expression - such as a threatening message to another student or a violent Web site – creates the likelihood of material disruption of the school's operations, students may face school discipline and criminal penalties.

11. Hingham takes bullying and harassment by computer very seriously. Students shall not use any Internet or other communication device to intimidate, bully, harass, or embarrass other students or staff members. Students who engage in such activity on school grounds or who engage in such activity off campus and create a material disruption of school operations shall be subject to penalties for bullying and harassment as contained in the student handbook, as well as possible criminal penalties.

In the event of a claim that a student has violated this policy, the District will provide the student with notice and an opportunity to be heard in the manner set forth in the student handbook.

Best Practices

DO be polite and use appropriate language in your network communications. Email, however informal, is subject to the same rules of etiquette as the more traditional forms of correspondence. DO NOT get abusive in your messages to others. Do not swear, use vulgarities or any other inappropriate language.

DO NOT reveal your personal address or phone number, or that of other students or colleagues online or elsewhere on the network.

DO respect the privacy of others. All communications and information accessible via the network should be assumed to be private property.

DO NOT use another individual's account without written permission from that individual. To do so constitutes fraud.

DO logoff a computer workstation when you are through using that system. This is the best way to safeguard your work and your network identity.

DO NOT use the network in such a way that you would disrupt the use of the network by other users.

DO help the system run smoothly. If you feel you can identify a security problem on the network or the Internet, notify a system administrator. DO NOT demonstrate the problem to other users.

DO NOT open email attachments unless you know the source and expect the file.