AMHERST-PELHAM PUBLIC SCHOOLS - REGULATIONS AND PROCEDURES

APPROPRIATE USE OF TECHNOLOGY

I7 – Instruction

The Districts' electronic resources—including, but not limited to, computers, electronic devices, and Internet access—allow users access to local, national, and international sources of information and collaboration vital to intellectual inquiry and democracy, and are intended solely for educational purposes. Every user has the responsibility to respect and protect the rights of every other user in the school communities and on the Internet. Account holders are expected to conduct themselves in a responsible, ethical, and legal manner, in accordance with both school and district policies, rules, regulations and guidelines and the laws of the Commonwealth of Massachusetts and the United States.

Use of computer networks and the Internet are revocable privileges dependent upon compliance with school/district policy. A user's failure to comply with policy shall result in limited network/Internet access, suspension of access, and/or other disciplinary action.

This procedure is based upon the Districts' Appropriate Use Policy (IJNDB) and shall serve to guide student and staff use of the Internet and technology. The guidelines are intended to advance the educational goals of the Districts by improving access to unique resources and partnerships, and by improving learning and teaching through research, teacher training, collaboration and distribution of successful education practices, methods and materials.

The Districts also seek to ensure a healthy and appropriate use of Internet resources by making provisions to:

- Prevent access to inappropriate matter or harmful materials on the Internet by minors
- Maintain the safety and security of minors when using electronic mail or Internet-based communications
- Prevent unauthorized access to the Districts' network and technology, including "hacking" and other unlawful activities
- Prevent unauthorized disclosure, use and dissemination of personal information regarding minors

The District acknowledges the potential that outside the school/district network, users may access, intentionally or innocently, inappropriate material that is inconsistent with the Districts' educational purpose. While violations of school/district policy are cause for concern and will be managed as required by policy and law, we maintain the educational advantages of using the Internet outweigh the disadvantages. It is recommended that parents and guardians establish standards of use of electronic media that is consistent with school/district policy.

The Districts' respect each family's decision whether their child should or should not have access to the Internet. Students will be given an account on the Districts' network and access to the Internet unless a parent or legal guardian submits a signed request refusing access.

User Provisions

A. All users: Students, staff and faculty shall not:

1. Use the network to access and/or transmit material in violation of any U.S. or Commonwealth law, including copyrighted material.
2. Access, download, display, transmit, produce, generate, copy or propagate any material that is obscene or pornographic material; advocates illegal acts; contains ethnic slurs, or racial epithets; or discriminates on the basis of gender, national origin, sexual orientation, race, religion, ethnicity, handicap or age.
3. Degrade, damage or disrupt equipment or system performance.
4. Gain unauthorized access to network resources.
5. Permit or authorize any other person to use their name or login password. 6. Use an account of any other person or vandalize another user's data.

7. Waste electronic storage space by saving unnecessary files or programs.
8. Download, install, load or use programs without written permission of a technology administrator.

9. Use the Internet for personal commercial purposes or for political lobbying.
10. Use inappropriate, offensive, foul or abusive language.
11. Harass or annoy any other party with obscene, libelous, threatening or anonymous messages, objectionable information, images or language.
12. Forward chain letters.
13. Forward e-mail messages of broad interest—including virus alerts and jokes—to the entire school community (see number 5 below).
14. Knowingly make use of pirated software or violate software licensing agreements.
15. Engage in the practice of "hacking" or knowingly engage in any other illegal activity with using the network.

Additionally, students, staff and faculty must:

- Use the Internet and other electronic resources only for legitimate educational purposes.
- Respect commonly accepted practices of Internet etiquette including, but not limited to, use of appropriate language.
- Be aware of potential security risks at all times and take all reasonable steps to minimize risks by, at minimum, logging off the network when a computer is unattended and reporting all unauthorized use of one's account to a technology administrator.
- Avoid bulk e-mailing
- Forward all e-mails of broad interest, such as virus alerts, to a technology administrator for appropriate distribution to the entire school community.
- Treat all computer areas and equipment with the utmost care and respect

B. Students: Students may access the Internet with adult permission; student use of electronic resources is restricted to teacher-approved projects and research. Students should notify a teacher or technology administrator immediately if they come across inappropriate content. In addition, students should not use the Internet to give out personal information (such as a home address, telephone number, or picture) about themselves or other students.

Network and Internet Monitoring

The Districts have software and systems in place that monitor and record all Internet usage. The Districts' security systems are capable of recording specific internet use, including by not limited to each web site visit, chat, newsgroup, e-mail message, and file transfer into and out of our internal networks for each user. Given reasonable cause, the District will intermittently monitor Internet traffic and other usage of electronic resources. Users should have no expectation of privacy when browsing the web, sending or receiving email, or using other electronic resources.

Filtering

In accordance with the Children's Internet Protection Act (CIPA), passed by the U.S. Congress in January 2001 (Public Law 106-554), the Districts' shall employ filtering software to block access to inappropriate content on all computers with Internet access. The Districts' and the schools certify that a policy of Internet safety and technology protection measures shall be enforced. Users are restricted from accessing visual depictions of subject matter that is obscene, pornographic, child pornographic or harmful to minors. In compliance with CIPA the Districts and the schools shall, in furtherance of this policy of Internet safety, monitor the online activities of minors.

Users should be aware that filtering software will not block ALL inappropriate web sites. Users should report all inappropriate sites not blocked by filters to a teacher or school/technology administrator for appropriate action. Filtering software may be disabled for users 18 and over by a technology administrator for legitimate research purposes.

E-mail

School and District resources for electronic communication shall be used for educational purposes. It is likely that incidental and occasional personal use of electronic mail may occur, though such use should be limited. These messages will be treated no differently from other messages on the network. Prohibited electronic communications include, but are not limited to:

1. Use of electronic communications to send copies of documents in violation of copyright laws.

2. Use of electronic communication systems to send messages access to which are restricted by laws and regulations.
3. Use of electronic communications to intimidate others or to interfere with the ability of others to conduct school/district business.
4. Constructing electronic communications to they appear to be from someone else.

Software policies

A. Supported software
Software upon which the District has standardized will be given priority in terms of installation, troubleshooting and training. Decisions made regarding the selection and purchasing of computer software for instructional programs must be made in accordance with Amherst-Pelham School District Regulations and Guidelines. [See "Operations: Instructional Materials Selection, p. 76.] Specifically, secondary departments and programs "have the major responsibility to select basic instructional materials and to recommend their purchase for the school system [to the principals and] through the directors to the Superintendent." The Information Systems department mustd be consulted before any software purchase.

B. Other software
Installation, troubleshooting and training for all other software used by faculty, staff and students will be supported as time permits. Software to be used in the curriculum or in a lab environment must be purchased in quantities sufficient to satisfy manufacturer licensing requirements, and must be owned by the school/district. Single copies of software are considered evaluation copies and will not be supported, installed on multiple computers, or made available from the network to multiple computers. The district supports the use of free and open source software (FOSS), as long as it is compatible with the network and computers. Every effort will be made to accommodate FOSS, but the Information Systems department cannot support such software.

C. Unsupported software
Software which makes the computers and network harder to maintain and support and which offers little or no benefit over comparable software will not be supported. Please do not install unsupported software, including downloaded freeware or shareware, on your computer.

D. Downloaded software
Downloaded software is not generally supported by the District. If downloaded software is determined by the Technology Department to become problematic, the software may be removed or the computer/device may be wiped/re-imaged.

Web pages

A. General guidelines for student, teacher & classroom sites

1. Student pictures and work Use of student photos on any web page is to be at the discretion of individual schools and Districts. In all cases, however, a signed release form must be on record at the school before a student's photo can be placed on a web page, and only first names will be used with either pictures or school work.

2. Content Do not advertise, endorse or link to any product or organization whose primary function is not to disseminate educational content (e.g., commercial enterprises or political groups). Certain fundraising information and links may be allowed, such as "shopforschool.com" or "marketday.com" and certain exceptions may be made for commercial entities who have significantly contributed to the school community (e.g., Verizon or Microsoft). These company links are allowed at the discretion of appropriate school administrators; please see school- and district-specific provisions at the end of this document for more information. In all cases, exceptions may be made when links to commercial or political groups are provided for legitimate educational purposes—for instance, links to the sites of political parties for civics courses, or links to commercial entities for media literacy courses. Proof your content and use a spell checker before posting. As an educational institution with a potentially broad audience, it is incumbent upon us to have grammatically correct content. Viewers often have high expectations and we must maintain a high level of accountability to our community.

5. Copyright issues Use of copyrighted material conforms to the "fair use" test (http://www.benedict.com/basic/fairuse/fairtest.htm) and that all copyrighted material on your site is appropriately credited.