Electronic Resources Acceptable Use Procedures

A joint document drafted by the Technology in Education Partnership of Greater Franklin/Hampshire Counties

(School and district specific policies are appended to the end of this document)

Adopted by the following parties:

Amherst School District
Amherst-Pelham Regional School District
Franklin County Technical School
Frontier Regional and Union 38 School Districts
Gill-Montague Regional School District
Greenfield Public Schools
Hadley Public Schools
Hawlemont Regional School District
Mohawk Trail Regional School District
Northampton Public Schools
Orange Elementary Schools
Pelham School District
Pioneer Valley Regional School District
Ralph C. Mahar Regional School District
Rowe Elementary School

Table of Contents

I. Introduction

II. General Provisions
   A. Network and Internet monitoring
   B. Filtering

III. User-specific Provisions
   A. All users
   B. Students

IV. Electronic Communication

V. Software
   A. Supported software
   B. Other software
   C. Unsupported data, media and software

VI. Data Storage and Backup

VII. Hardware
   A. Use of equipment other than that owned by the school/district
   B. Wiring of network devices

VIII. Web Pages
   A. General guidelines for student, teacher & classroom sites
      1. Posting
      2. Disclaimers
      3. Student pictures and work
      4. Content
      5. Copyright issues

IX. School and District Specific Procedures

I. Introduction

This document is a joint effort of the Franklin and Hampshire County public schools, adopted by the school superintendents and technology coordinators/administrators for the purpose of guiding appropriate use of technology in education. The electronic resources at the public schools in Franklin and Hampshire County are provided by and in consonance with their mission to:

- Improve education for all students through access to unique resources and partnerships;
- Improve learning and teaching through research, teacher training, collaboration and distribution of successful education practices, methods and materials.

In addition, we seek to ensure a healthy and appropriate use of technology resources by making provisions for:

- Prevention of access by users to inappropriate matter on the Internet;
- The safety and security of users when using electronic mail, chat rooms, and other forms of direct electronic communications;
- Prevention of unauthorized access, including “hacking” and other unlawful activities;
- Prevention of unauthorized disclosure, use and dissemination of personal information regarding minors; and
- The design of measures to restrict minors’ access to harmful materials; and
- Prevention of any and all inappropriate or illegal use.

Our electronic resources—including, but not limited to, computers 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 the rights of every other user in our school communities and on the Internet. Users are required 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.

The potential exists, outside the school/district network, for users to access inappropriate material. A user may intentionally or innocently access material inconsistent with our educational purpose and policies. While violations of school/district policy are cause for concern, we maintain the educational advantages of using the technology outweigh the disadvantages. It is the burden of parents and guardians to establish standards of use of electronic media consistent with school/district policy and to ensure that users comply with established policy. We respect each family's decision whether their child should or should not have access to the Internet. Parents should notify the school in writing if they do not want the student

to use the Internet. The use of electronic resources is at the discretion of the schools/districts according to their individual electronic policy.

The following explains the TEP's common policies for acceptable use of the schools' and districts' technology. Policies specific to individual schools and districts are at the end of this document. Use of computer networks and the Internet are revocable privileges dependent upon compliance with school/district policy and these procedures. A user's failure to comply with policy shall result in limited network/Internet access, suspension of access, and/or other disciplinary action up to and including termination or expulsion.

II. General Provisions

Greater Franklin County schools have established certain protocols to ensure the safety of our school communities, the security of computer networks, and compliance with applicable law. All users should be aware of the following provisions:

A. Network and Internet monitoring

Most schools and/or their vendors have software and systems in place that monitor and record all Internet usage. Most security systems are capable of recording each web site visit, chat, newsgroup, e-mail message, and file transfer into and out of our internal networks for each user. We reserve the right to intermittently monitor Internet traffic and other usage of electronic resources, for instance, by tracking destination URLs of individual users. Users should have no expectation of privacy when browsing the web, sending or receiving e-mail, or using other electronic resources.

B. Filtering

In accordance with the Children's Internet Protection Act (CIPA), passed by the U.S. Legislature in January 2001 (Public Law 106-554), our schools shall employ filtering software to block access to inappropriate content on all computers with Internet access. Our schools and districts 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 are obscene, pornographic, child pornographic or harmful to minors. In compliance with CIPA, our schools and districts shall, in furtherance of this set of Acceptable Use Procedures regarding] Internet safety, monitor the online activities of users.

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

Our schools and districts cannot be held responsible for misuse of material downloaded from any online service, or for inappropriate or sexually explicit material being obtained through the network.

III. User-specific Provisions

A. All users

Students, administrators, 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; advocates illegal acts; contains ethnic slurs or racial epithets; or discriminates on the basis of gender, national origin, sexual orientation, race, color, ancestry, religion, handicap or age.
3. Degrade, damage or disrupt equipment or system / network performance (for example excessive bandwidth use that disrupts the network for other users).
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 the technology coordinator/administrator.
9. Use the Internet [even if they have a second job while not at school????] 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 in the section "Students, staff and faculty must").
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 using the network.
16. Engage in any other inappropriate use of the system.

Students, staff and faculty must:

1. Use the Internet and other electronic resources only for legitimate educational purposes.
2. Respect commonly accepted practices of Internet etiquette including, but not limited to, use of appropriate language.
3. 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.
4. Avoid bulk e-mailing
5. Forward all e-mails of broad interest, such as virus alerts, to a technology administrator for appropriate distribution to the entire school community.
6. Treat all computer areas and equipment with the utmost care and respect
7. Abide by this procedure and specific school policy

B. **Students**

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

IV. Electronic Communication

School and district resources for electronic communication shall be used for educational purposes. Incidental and occasional personal use of electronic mail may occur when such use does not generate a direct cost for the district, but such 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 appear to be from someone else.
5. Obtaining access to the files or communications of others for the purpose of satisfying idle curiosity, with no substantial school/district business purpose.
6. Users will conform to the rules of e-mail archiving and document retention.
7. Any other communication in violation of this policy or the specific school policy.

V. Software

A. Supported software

Software which the District has standardized will be given priority in terms of installation, troubleshooting and training. A list of standardized and supported software, and other software owned by the district, will be updated from time to time and made available for viewing at a location designated by the superintendent, principal, or technology administrator or his/her designated agent.

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 “lab packs” of sufficient quantities to account for the greatest number of simultaneous users or as site licenses, 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.

C. Unsupported data, media and 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. Do not install software, including downloaded freeware or shareware, on any computer. The technology coordinator/administrator reserves the right to uninstall unsupported media or reimage any computer as necessary. No personal data or files are to be stored on the local hard drive of any computer. Please store data and files in your home directory.

VI. Data Storage and Backup:

The technology coordinator/administrator has the right to reimage any computer as necessary.

No personal data or files should be stored on the local machine.

The school/district makes every effort to run regular backups on data and e-mail hosted on its systems and networks; however, it cannot guarantee that in the event of data loss or catastrophic failure all information will be recovered.

VII. Hardware:

A. Use of equipment other than that owned by the school/district:

1. The school/district does not support equipment brought in from the outside by any user.
2. The technology coordinator/administrator has the right to confiscate any outside equipment that interferes with operation of the system/network.
3. The school/district is not responsible for damage to or loss of equipment brought in from the outside.
4. Permission to set up any outside equipment on school premises must be given in advance by the technology coordinator/administrator or his/her designated agent.
5. Permission must be granted for use of electronic devices not owned or provided by the school/district.

B. Wiring of network devices:

Any wiring of computers and peripherals must be done to in accordance with local and state building codes. The connectivity requests should be made through the IT department. The IT department is solely responsible for this process.

VIII. Web Pages:

A. General guidelines for student, teacher & classroom sites

1. Posting

All web pages produced by faculty or staff that reference or depict the school/district are assumed to be school- or district-owned educational resources, created for the sole purpose of education, and shall be posted on a school-maintained web site, with the exception of school-authorized sites whose purpose is to simplify the process by which a page/site is posted. All student web sites/pages must be approved by authorized school personnel for posting prior to being posted.

2. Disclaimers

If a user's home page is housed on a school/district server, but has links to sites/pages which are *not* housed on a school/district server, the user must include the following disclaimer:

"The _____ District is not responsible for any content which is not hosted on our servers"

Any school-related web page produced by staff but not housed on the school web site must be posted to an authorized site and must include the following disclaimer:

"The contents of this site/page express the views of the author(s) only and do not necessarily express the views of the _____ School District."

The school/district is not responsible for content on school-related web sites not housed on our site or on another authorized site.

3. Student pictures and work

According to federal and state law, student personally identifying images and educational information cannot be posted on the web without prior written permission by the appropriate individual.

4. 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**

   Make certain that 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.

IX. School and District Specific Procedures