Tri-Valley Central School District

34 Moore Hill Road • Grahamsville, New York 12740

Phone (845) 985-2296 Thomas W. Palmer, Superintendent

Policy Revision History
September 1997
May 2001
June 2005
March 2009

BOARD POLICY -INSTRUCTION -8360
Acceptable Use of District's Information Technology Network

ACCESS TO NETWORKED INFORMATION RESOURCES

With the rapidly evolving technologies throughout the modern work place, the Board recognizes that individuals will shift the ways they gather and share ideas, transmit and receive information, and communicate with others. Emerging technologies will alter instruction and student learning. The Board supports access by students to rich information resources along with the development by staff of appropriate skills to analyze and evaluate such resources. In a free and democratic society, access to information is a fundamental right of citizenship.

Electronic information sources and networked services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. In the past, instructional and library media materials could usually be screened--prior to use--by committees of educators and community members intent on subjecting all such materials to reasonable selection criteria. Board Policy 8110 requires that all such materials be consistent with District-adopted guides, supporting and enriching the curriculum while taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students. As the Internet links fileservers around the world, electronic information resources, which have not been screened by educators for use by students of various ages, are readily available. As staff members and students are connected to the global community, their use of new tools and systems brings new responsibilities as well as opportunities.

To these ends, the Tri-Valley Central School (District) is providing employees and students with access to the **District's Information Technology Network (Network)**, which includes its computers, networks, Intranet access, Internet access, e-mail accounts, telephones, voice mail, and any other means of electronic communication technology known or hereafter developed. This Policy will govern all use of the Network. Student use of the system will also be governed by the Student Code of Conduct. Employee use will also be governed by District policy and the Professional Agreement between the Tri-Valley Teachers' Association and the Tri-Valley School District.

All Network users will be given a copy of this Board policy, and, on an annual basis prior to the start of the school year, all Network users (except students in grades PK through 2) will be required to sign a "Network Use Agreement" **prior to using any aspect** of the District's Network. Parents/guardians will be required to sign **all** student Agreements.

A. The Purpose of the Network

1. The purpose of the Network is:
   a. to assist in preparing students for success in life and work in the 21st Century by providing them with electronic access to a wide range of information and the ability to communicate with people throughout the world; and
   b. to support and extend classroom activities, professional or career development, and limited high-quality self-discovery activities, at the discretion of the immediate supervisor.
2. Additionally, the Network will be used to increase District intra-communication, enhance productivity, and assist District employees in upgrading their skills through greater exchange of information with their peers.
3. The Network allows the District to share information with the local community, including parents/legal guardians, social service agencies, government agencies, and businesses.

Access to the District's Network is provided solely for educational purposes and research consistent with the District's mission and goals.

B. Services Provided through Network

1. **Internet**: The Internet and its interactive capabilities provide access to a wide range of information in the form of text, graphics, photographs, video, and sound from throughout the world. The Internet is a valuable educational research and communication tool for students and employees.
    a. All students will have access to pre-approved links on the Internet ("Links Access"). Such links will be provided by the teachers or other District staff members after careful review. Students in grades PK-6 will not be allowed to use search engines or type in URLs. Parents/legal guardians may specifically request that their child(ren) not be provided such Links Access by notifying the Building Principal in writing. Parents/legal guardians must renew their request on an annual basis, prior to the start of each school year.
    b. Students in grades 7-12 may be granted additional access to networked computer services such as the Internet ("Search Access") if they complete Network Orientation with the building librarian. Students are required to comply with the requirements and instructions of supervising staff members (i.e., what one teacher may permit, another teacher may not). Parents/legal guardians may specifically request that their child(ren) not be provided such Search Access by notifying the Building Principal in writing. Parents/legal guardians must renew their request on an annual basis, prior to the start of each school year.
    c. All employees will have access to the Internet.
2. **Electronic Communication**: Electronic Communications (including but not limited to e-mail, instant messaging, telephone services, and other means of communication known or hereafter developed) will allow employees and students to communicate with people throughout the world.
    a. **Individual E-mail Accounts for District Employees** will be provided to District employees upon completion of e-mail training. These accounts will be monitored for their educational use and may be terminated. Employees will be able to subscribe to mail lists to engage in group discussions that are relevant to educational subjects or their professional/career development. The District relies on e-mail as a primary tool for communication. All staff members are responsible for checking and reading messages daily.
    b. **Individual School E-mail Accounts for Students** will be provided to students in grades 9-12 for class or extracurricular activities, and may be provided to students in other grades when requested by a teacher.
    c. **Other Forms of Electronic Communication** ("Other Communication Access") will be allowed for students at the discretion of the supervising staff member. Other Communication Access may include, for example, a class-specific chat room, a classroom blog, user of resources available on a teacher's homepage, online classes, posting a finished product (such as a student newspaper) on the District website, etc. All Other Communication Access must be monitored by the supervising staff member. Parents/legal guardians may specifically request that their child(ren) not be provided such Other Communication Access by notifying the Building Principal in writing. Parents/legal guardians must renew their request on an annual basis, prior to the start of each school year.
    d. **Telephone Services**: All teachers and office employees will be provided with a voice mail account.
    e. **911 Calls** can be made from any phone on the Network.
3. **Remote Access:** In its discretion, the District may make remote access available to provide users off-campus access to District Network resources.
4. **File Transfer Protocol (FTP):** FTP allows users to download large files and computer software. This will only be available upon special request from the District Director of Technology.
5. **Active Restriction Measures**: The District will utilize filtering software or other technologies in an effort to prevent Network users from accessing visual depictions that are: (i) obscene; (ii) child pornography; or (iii) harmful to minors. Use of such software and technologies cannot, however, guarantee that all inappropriate sites will be blocked. The District will also monitor the online activities of Network users, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material which is inappropriate for minors. Internet filtering software or other technology-based protection systems may be disabled by a teacher or school administrator, as necessary, for purposes of a staff member's bona fide research or other educational projects; such filters may only be disabled for students by the Director of Technology, or his/her designee, at the request of the supervising teacher/administrator.

C. Access to the Network Services

1. **Guest Accounts:** Guests (i.e., anyone other than District students and employees) may receive an individual account for the Network with the approval of an administrator if there is a specific, District-related purpose requiring such access. Use of the system by a guest must be specifically limited to the District-related purpose. Guests will be required to complete a "Guest TVCS Network Use Agreement" and, if the guest is a student (e.g., Districts may allow home schooled students to obtain access through the Network), the signature of a parent/guardian will also be required. E-mail accounts will be provided to guests only when needed for an in-service course or for a special need and approved by an administrator.

2. **Personal Equipment:** Network users may not access the Network using their own personal equipment (laptops, PDAs, etc.) in school, unless they have the express written approval of the Director of Technology. All personal equipment must meet certain requirements specified by the District in order to be allowed a direct connection to the Network.

D. District Responsibilities

1. The Director of Technology will:
   a) oversee the Network;
   b) coordinate activities with each Building Principal;
   c) work with the MHRIC and/or Sullivan County BOCES as necessary;
   d) maintain executed user agreements;
   e) maintain a list of students who are not allowed to access the Internet; and
   f) report inappropriate behavior to the student's principal/staff member's supervisor who will take appropriate disciplinary action. Violations may result in a loss of access to the Network and/or disciplinary action, (if applicable) consistent with the Code of Conduct or the Professional Agreement between the Tri-Valley Teachers' Association and the Tri-Valley School District. When applicable, law enforcement agencies may be involved.

2. The Building Principal will:
   a) serve as the building-level coordinator for the Network;
   b) approve building-level activities;
   c) ensure teachers receive proper training in the use of the Network and effective use of telecommunication and electronic communication;
   d) ensure that the teachers understand the requirements of this Board policy;
   e) establish a system to ensure adequate supervision of students using the Network; and
   f) be responsible for interpreting this Policy at the building level.

3. The Director of Technology will establish a process for setting-up individual and class accounts, set quotas for disk usage on the system, establish a retention schedule, establish a District virus protection process, and perform other duties as necessary.

The responsibilities set forth in paragraphs 1-3 above are intended to be illustrative only, and are not necessarily an exhaustive list.

E. Employee Responsibilities

The Board encourages staff to make use of telecommunications to explore educational topics, conduct research, and contact others in the educational world. The Board anticipates that the new systems will expedite the sharing of effective practices and lessons across the District and will help staff stay on the leading edge of practice by forming partnerships with others across the nation and around the world.

1. Employees will learn to use electronic mail and telecommunications tools and apply them in appropriate ways to the performance of tasks associated with their positions and assignments. Toward that end, the Board directs the Superintendent to provide staff with appropriate training.

2. Employees are expected to communicate in a professional manner consistent with federal and state laws governing the behavior of school employees, with federal laws governing copyrights and other intellectual property, with federal and state laws concerning student rights of privacy, and with standards of acceptable employee conduct that apply to any aspect of job performance.

3. Employees will be issued a log-in name/account and password. Passwords should be changed periodically. Employees should never share their password or account with anyone. They have full responsibility for the use of their account and can be held responsible for any policy violations that are traced to their account. Staff will not allow anyone, including but not limited to students, to log into or use their account (including but not limited to e-mail).

4. Staff will subscribe only to high quality electronic discussion groups that are relevant to educational subjects or their professional/career development. Staff will limit their use of e-mail subscriptions and listservs and shall not subscribe to anything that is personal or non-school related.

5. Staff will inform students of their rights and responsibilities as users of the Network prior to allowing them access to that Network. Staff will tailor their instructions to the type of Network access granted to the students.

6. Before using the Internet with a class, teachers will check the list of students who are not allowed to participate in Internet activities and shall arrange for acceptable alternative learning activities for such children.

7. When using the Internet for class activities, teachers will select material that is developmentally and age appropriate for the students and that is relevant to the course objectives.

8. To determine the appropriateness of the material contained on or accessed through a site, teachers will preview all the materials and sites they require or recommend students access. Students in grades PK-6 will be provided Links Access and are not permitted Search Access.

9. Teachers will offer "home pages" and menus of materials which comply with Board guidelines listed in Board Policy 8110 governing the selection of instructional materials. These guidelines and lists of resources will assist students in channeling their research activities effectively and properly.

10. Staff members will only allow students to communicate electronically for educational purposes and all such communication will be monitored by a staff member.

11. Teachers will assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

The responsibilities set forth in paragraphs 1-11 above are intended to be illustrative only, and are not necessarily an exhaustive list.

F. Parental/Legal Guardian Notification and Responsibility

1. The District will notify the parents/legal guardians about the Network and the policies governing its use. The District's website contains links to information concerning student Internet safety.

2. All students may have classroom activities which include Links Access.

3. For a student in grades 7-12 to have Search Access to the Network, the student must complete Network orientation.

4. Section M of this Policy both specifies prohibited uses of the District's Network and explains restrictions on accessing inappropriate material. Parents/legal guardians should instruct their child(ren) if there is material that they think would be inappropriate for their child(ren) to access, even if otherwise permitted by District policy. The District assumes no responsibility for monitoring and enforcing a wide range of social values in student use of the Internet; rather, it will enforce District policy regarding Network use.

The responsibilities set forth in paragraphs 1-4 above are intended to be illustrative only, and are not necessarily an exhaustive list.

G. Student Responsibilities

1. Access to the Network is a privilege, not a right. Access entails responsibility and inappropriate use may result in the suspension or revocation of that privilege.

2. Students are responsible for good behavior on the Network just as they are in a classroom or a school hallway. General school rules for behavior apply.

3. Students will immediately notify a teacher or the Director of Technology if they have identified a possible security problem. They must not go looking for or share security problems, because this may be construed as an illegal attempt to gain access.

4. Students are responsible for their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should students provide their password to other persons, other than their parents/legal guardians. Students have full responsibility for the use of their account and can be held responsible for any policy violations that are traced to their account.

5. If students mistakenly access inappropriate information, they should immediately tell their teacher or another District employee.

6. The District fully expects that students will follow their parents'/legal guardians' instructions regarding access to, and refraining from accessing, certain material on the Internet.

The responsibilities set forth in paragraphs 1-6 above are intended to be illustrative only, and are not necessarily an exhaustive list.

H. District Limitation of Liability

The District makes no warranties of any kind, either express or implied, for the access, functions or services provided by or through the Network. The District is not responsible for the accuracy, quality, availability, nature or reliability of the service and/or information obtained through or stored on the Network. Users of the District's Network use the Network and the information available thereon at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided. The District will not be responsible for any damages suffered by the user, including, but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by any reason, including, but not limited to, the District's own negligence or the errors or omissions of any user. The District also will not be responsible for unauthorized financial obligations arising through the unauthorized use or access to the District's Network.

I. Due Process

1. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any illegal activities conducted through the Network.

2. In the event there is an allegation that a student has violated this Policy, the student will be notified of the alleged violation and given an opportunity to present an explanation before the Director of Technology or his/her designee. All disciplinary action taken will be in accordance with the Code of Conduct.

3. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of other school policies, the violation will be handled in accord with those policies.

4. Employee violations of this Policy will be handled in accord with District policy and the Professional Agreement between the Tri-Valley Teachers' Association and the Tri-Valley School District.

5. Any District administrator may terminate the account privileges of a guest user at any time for any reason.

J. No Expectation of Privacy & Monitoring Usage

Network users have no expectation of privacy in anything they create, store, access, send or receive on the Network (including but not limited to, documents, text or instant messages, e-mails, and any other means of communication known or hereafter developed, whether of a business or personal nature). The District has the right, but not the duty, to monitor any and all of the aspects of its Network to the extent such monitoring is not inconsistent with applicable laws. ***Users hereby consent to such monitoring by the District, without further notices***. The District's Network may create back up information and communications and, as such, information and communications may be retrieved and accessed. Users shall be responsible for their activities on the Network. Teachers and other District staff have access to monitor student Network activity.

K. Copyright and Plagiarism

1. District policies on copyright will govern the use of material accessed through the Network. Because the extent of copyright protection of certain works found on the Internet is unclear, employees will make a standard practice of requesting permission from the holder of the work if their use of the material has the potential of being considered an infringement. Teachers will instruct students to respect copyright and to request permission when appropriate.

2. District policies on plagiarism will govern use of material accessed through the Network. Teachers will instruct students in appropriate research and citation practices.

L. District Web Site

1. **Web Sites & Web Pages In General**

a) **District Web Site**. The District maintains a Web site that presents information about the District.
b) **School or Class Web Pages**. Schools and classes may establish Web pages that present information about the school or class activities. Web pages must conform to the District guidelines.
c) **Extracurricular Organization Web Pages**. With the approval of the Building Principal, extracurricular organizations may establish Web pages. The principal will establish a process and criteria for the establishment and posting of material, including pointers to other sites, on these pages. Material presented on the organization's Web page must relate specifically to the organization's activities and will include only student-produced material. Organization Web pages must include the following notice: "This is a student's extracurricular organization Web page. Opinions expressed on this page shall not be attributed to the District." The Web master will have final approval before posting any web page on the District's Web server.

The content of the above-referenced types of "Web pages" will be referred to in this policy as "Web Content."

2. **Procedure Protocols for Web Site Management:** Web Content will promote and enhance educational opportunities and provide timely and appropriate information to the school community and beyond. Web Content will be consistent with the District's mission and goals and Board of Education policies.

3. **Oversight:** The Superintendent will designate staff member(s) who will be responsible for monitoring the accuracy and consistency of Web page content. A curator has the right to view, edit, modify, or delete without notice any material deemed inappropriate. Access to the administrative area is limited to authorized personnel only. The creation of Web sites by students must be done under the supervision of a professional staff member.

4. **Content:** A Web site is only as good as the information it contains. At a minimum, Web Content will be:
   - Free of spelling and grammatical errors;
   - Free of copyrighted material, unless an appropriate license has been obtained for use;
   - Accurate, concise and well-written;
   - Proofread in web browser to insure it has been edited correctly;
   - Reviewed and updated regularly;
   - Posted with a "show date" and "hide date"; and
   - Consistently formatted for clarity.

   The District reserves its right to impose additional requirements and restrictions for Web Content.

5. **Security & Confidentiality:** The privacy of students and employees will be respected.

.

   - The District will not include in Web Content any students' names or initials, photos or other information on individual students without first verifying that parental consent has been given. A child's name will never be linked with a photo.
   - An employee's photos and information may be posted, unless the employee has provided the District's Director of Technology services with a signed, written request that such information not be posted on the District's website. Contact information for an employee will be restricted to school address, work phone number, and District e-mail address.
   - Publication of personal addresses, phone numbers, or e-mail addresses is prohibited.
   - Links to personal web pages and sites that contain inappropriate material are prohibited.

   Violation of these protocols may result in suspension or revocation of Network privileges.

6. **Tri-Valley Central School District Web Policy Guidelines:**

   a) **Storing Data:** All information entered in the administrative area is stored on a server. After the hide date, information is archived. It is a good idea, however, to retain copies of files and graphics that support your Web design in a separate folder on your own disk, hard drive, or district server. To prepare a document for downloading, first save it as a PDF file (Portable Document Format) then enter it into the Web site filing cabinet.

   b) **Text:**

      - When formatting, keep font, font size, and font color consistent throughout the section/building you are editing. Font specs must be consistent throughout a Teacher's Page or Web Site section. Use of color and size should be used only for emphasis and kept to a minimum.
      - To create one line of white space, use two carriage returns. Use of HTML to manipulate text and change formatting should be kept to a minimum. When using HTML, make sure to view the page in Internet Explorer and Netscape at a variety of screen resolutions to insure the code is valid.

Tip: *When possible, create content in a word processing program prior to using the cutting and pasting technique to enter data into administrative area.*

Tip: *Use only one space after periods, colons, exclamation points, question marks, quotation marks—any punctuation that separates two sentences.*

c) **Color:** By default, text is entered in black. Color may be changed by using the RTE, but should be used judiciously. Color should complement template. Graphics import in their original color. Changes should be made in graphic design programs such as Adobe Photoshop or Illustrator before importing.

d) **Graphics:** Images, photos and other graphics should be entered into the Image Icon Bank.
- Limit the number of graphics on a page.
- Save photos as jpegs and images as gifs.
- Image file size should be 200 K (kilobytes) or less.
- Limit the size of animated graphics.
- Check links to insure validity.

e) **Design:** "Just because you can, doesn't mean you should." Remember, not everyone's system has the capability to support fancy moving graphics or the time to load graphics-heavy pages. Long download time discourages visitors to your site.

M. Prohibited Uses

The following is an illustrative, not an exhaustive, list of prohibited activity concerning use of the District's Network. Violation of any prohibition of Network use may result in suspension or revocation of a user's access to the computer Network and/or other disciplinary action:

1. Using the Network to receive, transmit or make available to others obscene, offensive or sexually explicit material, material that advocates illegal acts, or material that advocates violence or discrimination towards other people (hate literature). A special exception may be made for hate literature if the purpose of such access is to conduct research and access is approved by both the teacher and the parent/legal guardian. District employees may access the above material only in the context of legitimate research;
2. Using the Network to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others, including but not necessarily limited to messages that violate the District's Anti-Harassment Policy (Policy #3000) and Sexual Harassment (Students) Policy (Policy #7560).;
3. Posting false or defamatory information about a person or organization, as applicable;
4. Revealing the personal address, telephone number or other personal information of oneself or another person;
5. Forging or attempting to forge e-mail messages;
6. Using the Network to send anonymous messages or files;
7. Attempting to read, delete, copy or modify the e-mail of other Network users and deliberately interfering with the ability of other Network users to send and/or receive e-mail;
8. Intentionally disrupting Network traffic or crashing the Network and connected systems;
9. Attempting to override Network security;
10. Attempting to gain, or gaining, unauthorized access to the Network or to any other computer system using the Network, or by gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems;
11. Engaging in practices that threaten the Network (including, but not limited to, installing personal or other software or using personal disks on the District's computers and/or Network without permission);
12. Violating regulations prescribed by the Network provider;
13. Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the District's computers or Network, without having property authorization, license and/or permission (as applicable) for such activity or use;
14. Stealing data, equipment or intellectual property;
15. Using another's account or password, or using without permission another's folders, work, or files;
16. Intentionally wasting limited resources;

17. Reposting a private message without the permission of the person who sent the message;
18. Posting chain letters or engaging in "spamming";
19. Using the Network for sending and/or receiving personal messages
20. Engaging in vandalism; vandalism is defined as any malicious attempt to harm or destroy the District's Network or related materials, data of another user of the District's Network or of any of the entities or other networks that are connected to the Internet (including but not limited to, creating, placing or spreading a computer virus on the Network);
21. Downloading large files;
22. Engaging in any illegal act;
23. Allowing students in grades PK -6 Search Access ;
24. Allowing any student to communicate on the Network unless there is an approved activity and the students are being monitored;
25. Using the District Network for commercial or financial gains or purposes or fraud; District acquisition policies will be followed for District purchase of goods or services through the Network;
26. Using the Network for commercial activity, including advertising;
27. Using the Network for unapproved fundraising purposes;
28. Using the Network for political lobbying;
29. Using the Network while access privileges are suspended or revoked; and/or
30. Using the Network in a fashion inconsistent with directions from teachers and other staff or supervisors, as applicable, and generally accepted proper etiquette.

ANY INDIVIDUAL WHO HAS QUESTIONS OR PROBLEMS WITH THE NETWORK SHALL CONTACT THE DISTRICT'S TECHNOLOGY DIRECTOR