HAMPTON TOWNSHIP SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF INTERNET

ADOPTED: June 23, 2004

REVISED: December 05, 2011

815. ACCEPTABLE USE OF INTERNET

1. Purpose

The Board supports use of the Internet and other computer networks in the District's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration.

For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the school District as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

2. Authority

The electronic information available to students and staff does not imply endorsement by the District of the content, nor does the District guarantee the accuracy of information received. The District shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The District shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

The District reserves the right to log, monitor, inspect, copy, review, and store, at any time, and without prior notice, any and all usage of the District Information Technology Resources, and any and all information transmitted or received in connection with such usage, including logging information that was created, accessed or transmitted using the District’s Information Technology Resources.

The Board establishes that network use is a privilege, not a right; inappropriate, unauthorized, and illegal use will result in cancellation of those privileges and appropriate disciplinary action.

Definitions

“Vandalism” is defined as any malicious attempt to harm or destroy equipment or data of another user, Internet or other networks; this includes, but is not limited to, uploading or creating computer viruses.

“Information Technology Resources” is defined as an all encompassing term that includes Technology, Software, and Internet.

“Internet” encompasses but is not limited to the following networks; lan (local area network), wan (wide area network), regional area network, intranet, extranet, www (world wide web) and associated technologies; email, web browsing, text/chat, social networking/media.

	"Network Guest" is defined as any individual who utilizes the District's Information Technology Resources via guest network access or the guest login process.
P.L. 106-554 Sec. 1732	The Board shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by students.
3. Delegation of Responsibility	The District shall make every effort to ensure that this resource is used responsibly by students, staff, and Network Guests.
PL 110-385	Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals. Training and professional development will occur on an as-needed basis. This training shall include educating students about appropriate online behavior, including interacting with other individuals on social networking websites or in chat rooms, as well as cyber bullying awareness and appropriate responses. Students, staff, and Network Guests have the responsibility to respect and protect the rights of every other user in the District and on the Internet. The building administrator shall have the authority to determine what is inappropriate use.
P.L. 106-554 Sec. 1711, 1721	The Superintendent or designee shall be responsible for implementing technology and procedures to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to: 1. Utilizing a technology protection measure that blocks or filters Internet access by students, staff, and Network Guests to certain visual depictions that are obscene, child pornography, harmful or determined by the Board to be inappropriate for use by students, staff, and Network Guests. 2. Maintaining and securing a usage log. 3. Monitoring online activities of students, staff, and Network Guests.
4. Guidelines	Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system. <u>Prohibitions</u> Students and staff are expected to act in a responsible, ethical and legal manner in accordance with District policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Illegal activity.
2. Commercial or for-profit purposes.
3. Non-work or non-school related work.
4. Product advertisement or political lobbying.
5. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
7. Access to obscene or pornographic material or child pornography.
8. Access by students, staff, and Network Guests to material that is determined to be inappropriate in accordance with Board policy.
9. Inappropriate language or profanity.
10. Transmission of material likely to be offensive or objectionable to recipients.
11. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
12. Impersonation of another user, anonymity, and pseudonyms.
13. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
14. Loading or using of unauthorized games, programs, files, or other electronic media.
15. Disruption of the work of other users.
16. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
17. Quoting of personal communications in a public forum without the original author's prior consent.

<u>Security</u>

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, the following guidelines shall be followed:

1. Students, staff, and Network Guests shall not reveal their passwords to another individual.
2. Users are not to use a computer that has been logged in under another student's or employee's name.
3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

<u>Consequences For Inappropriate Use</u>

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations; and theft of services will be reported to the

	appropriate legal authorities for possible prosecution. General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use. Vandalism will result in cancellation of access privileges. <u>Copyright</u>
P.L. 94-553 Sec. 107 Pol. 814	The uploading or downloading of materials to the network in violation of copyright law is prohibited. <u>Safety</u> To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc. Any District computer/server utilized by students, staff, and Network Guests shall be equipped with Internet blocking/filtering software.
P.L. 106-554 Sec. 1732 P.L. 94-553 Sec. 107 P.L. 106-554 P.L. 94-553 Sec. 107 P.L. 106-554 Sec. 1711,1721,1732 20 U.S.C. Sec. 6777 Board Policy 814	Internet safety measures shall effectively address the following: 1. Control of access by students to inappropriate matter on the Internet and World Wide Web. 2. Safety and security of students when using electronic mail, chat rooms, and other forms of direct electronic communications. 3. Prevention of unauthorized online access by students, including "hacking" and other unlawful activities. 4. Unauthorized disclosure, use, and dissemination of personal information regarding students. 5. Restriction of student’s access to materials deemed to be harmful to them.