HANOVER PUBLIC SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF INFORMATION TECHNOLOGY

ADOPTED: January 28, 1997

REVISED: April 26, 2012

815. ACCEPTABLE USE OF INFORMATION TECHNOLOGY

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. It is the intent of Hanover Public School District to promote responsible, ethical, and appropriate use of information technology and network resources.

With Internet and e-mail access comes the availability of material that may not be considered appropriate in a school setting. The district cannot regulate and monitor all the information received or sent by persons who use the Internet or e-mail; and the district cannot ensure that students who use the network, Internet or e-mail will be prevented from accessing inappropriate materials or sending or receiving objectionable communications. The district believes, however, that the availability and value of the Internet and e-mail far outweigh the possibility that users may procure inappropriate or offensive materials. Access to the district information technology and network resources is a privilege, not a right. Staff and students will be held accountable for noncompliance with this policy.

2. Authority

The district reserves the right to log, monitor, and review Internet, e-mail, and other network use of each user. This logging, monitoring, and review may be conducted without cause and without notice. Each user of a district computer or the district network, by the use thereof, agrees and consents to such logging, monitoring, and review and acknowledges that s/he has no right or expectation of confidentiality or privacy with respect to Internet, e-mail or other network resources. Users should expect that files stored on district servers or computers will not be private. An e-mail archiving system is utilized in the district.

24 P.S.
Sec. 4601 et seq
20 U.S.C.
Sec. 6777
47 U.S.C.
Sec. 254

The district employs the use of an Internet filter as a technology protection measure pursuant to the Children's Internet Protection Act. The filter may not be disabled or bypassed by students or other minors for any reason.

All students, administrators, and staff members who use the Internet, e-mail, and other network facilities must agree to and abide by all conditions of the policy. The district makes no warranties of any kind, whether express or implied, for the service it is providing.

The district is not responsible, and will not be responsible, for any damages, including loss of data resulting from delays, nondeliveries, missed deliveries, or service interruption. Use of any information obtained through the use of the district network is at the user's risk. The district disclaims responsibility for the accuracy or quality of information obtained through the Internet or e-mail.

The district assumes no responsibility or liability for any changes incurred by a user. Under normal operating procedures, there will be no cost incurred.

A user may not install any software onto local and/or network drivers or disks, unless s/he has the specific, prior written permission from the technology department.

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.

Users have the responsibility to respect and protect the rights of every other user in the district and on the Internet.

The administration shall have the authority to determine what is inappropriate use.

3. Delegation of Responsibility
   20 U.S.C. Sec. 6777
   47 U.S.C. Sec. 254
   47 CFR Sec. 54.520

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 for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the administration.

2. Maintaining and securing a usage log.

3. Monitoring online activities.

SC 1303.1-A
Pol. 249

4. Providing training to minors in appropriate online behavior. This includes behavior when interacting with other individuals on social networking websites, and in chat rooms, and cyberbullying awareness and response.

4. Guidelines

Procedures

Network accounts or access to the Internet will be used only by the authorized user for its authorized purpose. Network users shall respect the privacy of other users on the system. Account/Access will be granted to only those individuals who meet the following requirements:

1. Students must have read the Internet Access Agreement Form and indicate their agreement with its provisions by signing the signature page and returning it to the appropriate district authority. Students must have their parent/guardian sign the signature page indicating the parent's/guardian's acceptance of the policy and agreement of the terms of the policy and their consent to allow the student to access and use the network.

2. Students and employees must have received instruction on network access, use, acceptable versus unacceptable uses, network etiquette, and the consequences of abuse of privileges and responsibilities.

General Prohibitions

The use of the Internet computer network for illegal, inappropriate, unacceptable, or unethical purposes by students or employees is prohibited. The administration reserves the right to determine if any activity constitutes an acceptable or unacceptable use of the network. With respect to all users, the following are expressly prohibited:

1. Use in an illegal manner or to facilitate illegal activity.

2. Use for commercial, private advertisement, or for-profit purposes.

3. Use for lobbying or political purposes.

4. Use to infiltrate or interfere with a computer system and/or damage to data, files, operations, software or hardware components of a computer or system.

5. Hate mail, harassment, discriminatory remarks, threatening statements and other antisocial communications on the network.

Pol. 814	6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
Pol. 237	7. Use to access, view or obtain material that is obscene, pornographic, including child pornography, or harmful to minors.
	8. Transmission of material likely to be offensive or objectionable to recipients as determined by district administration.
	9. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
	10. Impersonation of another user, anonymity, and pseudonyms.
	11. Loading or using of unauthorized software or media.
	12. Disruption or distraction of the work of other users.
	13. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
	14. Quoting personal communications in a public forum without the original author's prior consent.
	15. Use of the name of the school district and use of written logos or web content provided by the district through its web site without the written permission of the Superintendent.
	16. Allowing an unauthorized person to use an assigned account.
	17. Creation and introduction of computer viruses, trojans, worms, and other malicious programs.
	18. Use of software or hardware to compromise or bypass network security.
SC 1303.1-A Pol. 249	19. Bullying/Cyberbullying.
	20. Use while access privileges are suspended or revoked.
	21. Any attempt to circumvent or disable the filter or any security measure.
	22. Use inconsistent with network etiquette and other generally accepted etiquette.

Student Prohibitions

1. Disclose, use or disseminate any personal identification information of themselves or other students.

2. Engage in or access chat rooms or instant messaging without the permission and supervision of a teacher or administrator.

Etiquette

Users are expected to abide by the generally accepted rules of network etiquette. These include but are not limited to the following:

1. Be polite. Do not become abusive in messages to others. General district rules and Board policies for behavior and communicating apply.

2. Use appropriate language. Do not swear or use vulgarities or other inappropriate language.

3. Do not reveal personal information such as addresses or telephone numbers of others.

4. Recognize that e-mail is not private or confidential.

5. Do not use the Internet or e-mail in any way that would interfere with or disrupt its use by other users.

6. Respect the rights of other users to an open and hospitable technology environment, regardless of race, sexual orientation, color, religion, creed, ethnicity, age, marital status or handicap status.

Security

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. Each user is required to report any security problems to the Technology Director. The problem is not to be demonstrated to other users. To protect the integrity of the system, the following guidelines shall be followed:

1. Users shall not reveal their passwords to another individual.

2. Users are not to use a computer or network resource that has been logged in under another User'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.

Consequences Of Inappropriate Use

24 P.S. Sec. 4604

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

Illegal use of the network: intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services will be reported to the appropriate legal authorities for possible prosecution.

The use of the Internet and network resources is a privilege, not a right. District administrative staff, along with the Technology Director, will deem what is appropriate and inappropriate use and their decision is final.

Pol. 218, 233, 317, 417, 517

Loss of access and other disciplinary actions shall be consequences for inappropriate use. Consequences of violations may include:

1. Suspension of information network access.
2. Revocation of information network access.
3. Suspension of network privileges.
4. Revocation of network privileges.
5. Suspension of computer access.
6. Revocation of computer access.
7. School suspension.
8. School expulsion.
9. Report of violation of local, state or federal laws to appropriate legal authorities.
10. Dismissal from employment.
11. Legal action and prosecution by the authorities.

Vandalism will result in cancellation of access privileges. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to:

1. Creating or spreading computer viruses, worms, trojans, and other malicious programs.

2. Compromising network security.

Copyright

17 U.S.C.
Sec. 101 et seq
Pol. 814

The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.

Safety

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.

All district computers/servers utilized by students and staff shall be equipped with Internet blocking/filtering software.

47 U.S.C.
Sec. 254
47 CFR
Sec. 54.520

Internet safety measures shall effectively address the following:

1. Control of access to inappropriate matter on the Internet and World Wide Web.

2. Safety and security when using electronic communications.

3. Prevention of unauthorized online access including “hacking” and other unlawful activities.

4. Unauthorized disclosure, use, and dissemination of personal information.

5. Restriction of minors' access to materials harmful to them.

References:

School Code – 24 P.S. Sec. 1303.1-A

PA Crimes Code – 18 Pa. C.S.A. Sec. 5903, 6312

Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.

U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq.

Sexual Exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256

Enhancing Education Through Technology Act – 20 U.S.C. Sec. 6777

Internet Safety, Children's Internet Protection Act – 47 U.S.C. Sec. 254

Children's Internet Protection Act Certifications, Title 47, Code of Federal Regulations – 47 CFR Sec. 54.520

Board Policy – 103, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 417, 517, 814