

District Regulation

2361 - ACCEPTABLE USE OF COMPUTER NETWORKS/ COMPUTERS AND RESOURCES

Section: Program
Date Created: November, 2014
Date Edited: November, 2014

The Hasbrouck Heights Public Schools are responsible for securing their network and **computing** systems to a reasonable and economically feasible degree against unauthorized access and/or abuse, while making these accessible for educational purposes to authorized and legitimate users. This responsibility includes informing users, both registered and unregistered, of expected standards of conduct and the disciplinary or legal consequences for not adhering to them. Any attempt to violate the provisions of this policy will result in disciplinary action, including, but not limited to, temporary revocation of user accounts and computer usage, regardless of the success or failure of the attempt. Permanent revocations and/or other disciplinary actions may be taken by an administrator. The users of the network and computer equipment are responsible for respecting and adhering to local, State, Federal and international laws. Any attempt to break those laws may result in litigation against the offender by the proper authorities. If such an event should occur, the administration will fully cooperate with the authorities to provide any information necessary for the litigation process.

A. General **Computing**

Once a user receives a User-ID/email to be used to access the network and computer systems, the user is solely responsible for all actions taken by the User logged on with that User-ID/email. The following actions are prohibited:

1. Applying for a User-ID/email under false pretenses.
2. Sharing your User-ID/email with another person. (If you share your User-ID/email with another person(s), you and that person(s) will be responsible for any abuse that may occur.)
3. Deleting, examining, copying, or modifying files and/or data belonging to other users without prior consent of the owner.
4. Attempting to evade or change resource quotas.
5. Impeding other users through mass consumption of system resources.
6. Using facilities and/or services for unauthorized purposes.

7. Any unauthorized, deliberate action which damages or disrupts a **computing** system or network, alters its normal performance, or causes a malfunction regardless of system location or time duration.
8. Must utilize their assigned school email account to communicate in reference to school business.

B. Electronic Mail

Electronic mail ("e-mail") is an electronic message sent by or to a user in correspondence with another person having e-mail access. A canceled account will not receive its mail. Users are expected to remove old messages in a timely fashion and the system administrators may remove such messages if not attended to regularly by the user. There is no expectation of privacy regarding emails.

When a user sends electronic mail (e-mail) his/her name and User-ID are included in each mail message. The user is responsible for all electronic mail from his/her User-ID. Therefore, the following are prohibited:

1. Forging or attempting to forge electronic mail messages.
2. Reading, deleting, copying, modifying or viewing without permission, other user's e-mail or the attempt to do so.
3. Sending inappropriate, harassing, obscene or threatening e-mail to another user or the attempt to do so.
4. Sending unsolicited junk mail, "for-profit" messages, chain letters, or other inappropriate material or the attempt to do so.

C. Network and **Computing** System Security

A user of the network is allowed to access only authorized networks of the computer systems attached to those networks, therefore, the following are prohibited:

1. Using systems and/or networks in an attempt to gain unauthorized access to remote systems.
2. Using systems or networks to connect to other systems evading the physical limitations of the local or remote system.
3. Decrypting system or user passwords.
4. Copying system files.
5. Duplicating copyrighted materials.

6. Attempting to "crash" network systems or programs.
7. Attempting to secure a higher level of privilege on network systems.
8. Willfully introducing computer "viruses", disruptive, or destructive programs into the network or into external networks.
9. Installing or removing any and all software.
10. Installing or removing any hardware.

The Hasbrouck Heights network and **computing** systems are expected to be used exclusively for education-related functions and applications. As the system administrators have access to all files, including e-mail files, users should have no expectation of privacy with respect to said files or e-mail. The system administrators will not normally inspect the contents of files or e-mail sent by one user to an identified addressee unless required to do so by law or policies of the Hasbrouck Heights School District, or to investigate complaints regarding files or e-mail which are alleged to contain defamatory, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material. Moreover, Administrators are obligated to cooperate fully with local, State, or Federal officials in any investigation concerning or related to e-mail transmitted on, or misuses of the network and **computing** systems.

D. District Website

The district does not permit its website to contain copyrighted material without proper authorization. Staff members and students must abide by the following guidelines when submitting material for use on a district website. Anyone with questions regarding these guidelines should check with the library media specialist in their building before proceeding with the collection of images and text for the website.

1. District Technology Director ensures compliance. The District Technology Director shall be in charge of monitoring compliance and ensuring that the district website does not contain unauthorized use of copyrighted material.
2. No unauthorized reproductions. The district website shall contain no reproduction of any material, such as logos, photos, artwork, graphics, or even clip art, without permission from the copyright owner. Student work may be published only if written permission is obtained from both parent and student.
3. Get permission before republishing materials from the web. Copyright law and district policy do not allow the use or republishing of text or graphics found on the web on district websites or file servers without explicit written permission. The failure of a site to display a copyright notice may not be interpreted as permission to copy the materials. Unless there is a clear statement that graphics and text are in the public domain, students and staff should

assume they are copyrighted and only the copyright owner may provide the permission for use. If the materials have been improperly and illegally displayed by a website, the manager of that website may not be considered a source of permission.

4. District website must contain proper credit for copyrighted materials. For each use of a copyrighted work, there must be a notice at the bottom of the district website page crediting the original author or creator and noting how and when permission was granted. The notice should also include the web address or URL of the original source, if applicable.
5. Give documentation of permission to school. Students and staff engaged in producing web pages must provide library media specialists with e-mail or hard copy permissions to file before the web pages are actually published. In the case of public domain documents, printed evidence must be provided to document the status of the materials.

E. Camera Policy

All students and staff members are prohibited from using cell phones, cameras, web cams, school computers or any form of audio or video recording device in the classroom or during any instructional time outside the classroom, to record, display, post or transmit any form of personally identifiable information about any district employee or student, unless written permission is given by the staff member or the parent of the student whose information is involved. Such information is defined to include, but is not limited to, names, street addresses, email addresses, voice recordings and photographs or video pictures. Whether on or off school premises, all students are also prohibited from using school computers, school computer networks, school websites or school email or Internet accounts to record, display, post or transmit any form of personally identifiable information about any district employee or student.

It shall also be a violation of this policy for any student or staff member to use privately or commercially owned devices, networks or websites to post, display or transmit personally identifiable information about school employees or students, if that information was obtained in the classroom, during an instructional session outside of the classroom, or during a school related activity.

F. Social Media

Social media can not be accessed during school hours.

Exhibit

PARENT OR GUARDIAN NETWORK RESPONSIBILITY CONTRACT

As the parent or guardian involved in the education of this student, I have read the Terms and Conditions for Access to the Hasbrouck Heights Public School District's electronic network and computer equipment. I understand that this access is designed for educational purposes and the Hasbrouck Heights School District has taken precautions to eliminate controversial

materials. However, I also recognize that it is impossible for the Hasbrouck Heights School District to restrict access to all controversial materials, and I will not hold the District, members of the Board of Education, or its employees responsible for materials acquired on the network or computer systems that do not pertain to the prescribed curriculum or course of study. Further, I understand that the inappropriate use of the network or computer equipment by my child could result in school discipline, and/or criminal and civil penalties. Further, I accept responsibility for any damages or injuries caused by my child's use of the network or computer equipment, either in school or outside of school, in a manner which violates the Terms and Conditions set forth in this agreement.

With this understanding, I hereby give permission to issue electronic network access for my child and certify that the information on this form is correct.

Parent or Guardian: _____
(Please Print)

Name of Student: _____
(Please Print)

Parent/Guardian Signature: _____

Date: _____

Exhibit

STUDENT NETWORK AND **COMPUTING** RESPONSIBILITY

I UNDERSTAND AND AGREE TO ABIDE BY THE TERMS AND CONDITIONS FOR ACCESS TO THE HASBROUCK HEIGHTS PUBLIC SCHOOL DISTRICT'S ELECTRONIC NETWORK ACCOUNT AND COMPUTER EQUIPMENT. I FURTHER UNDERSTAND THAT ANY VIOLATIONS OF THE REGULATIONS ARE UNETHICAL AND MAY CONSTITUTE A CRIMINAL OFFENSE. MOREOVER, I UNDERSTAND THAT ANY VIOLATION OF THE GUIDELINES AND REGULATIONS COULD RESULT IN THE REVOCATION OF MY ACCESS RIGHTS, THE IMPOSITION OF SCHOOL DISCIPLINE, CRIMINAL PROSECUTION AND OTHER LEGAL ACTION.

Name of Student User: _____
(please print)

User Signature

Date