INTERNET/NETWORK USE REGULATIONS

Philosophy: It is the philosophy of the Hicksville Public Schools that the integration of technology with the curriculum is an essential part of instruction. At the same time, there is an inherent responsibility on the part of users to conduct themselves in an appropriate and considerate manner when using this medium. The Internet contains a rich array of educational content as well as information that is illegal or inappropriate for children. Therefore, Internet resources are filtered for inappropriate content, students are educated about Internet safety and appropriate online behavior, and student use is monitored and supervised by staff. However, the security, accuracy and quality of information that is available through our network cannot be guaranteed. While the guidelines that follow have been developed to ensure responsible use of our computer network and the Internet, we respect each family's right to deny independent Internet use by their children in school.

Parent/Guardian Option: A parent/guardian may deny their child independent access to the Internet at any time by submitting a letter to the school. However, teacher-directed Internet activities are part of our curriculum and not subject to parent/guardian authorization. Such activities may include the use of various online educational Web sites and services that may require students to set up individual user accounts, with the minimum required personal information, solely for the purpose of accessing such services in connection with approved classroom instruction. Unless a parent/guardian denies such access for their child, students will be permitted to set up their accounts, with the consent of their teachers, in accordance with the Children's Online Privacy Protection Act.

The following rules and regulations govern the use of the district's computer network system and access to the Internet and are intended to include the use of District e-mail, whether accessed remotely or via District computer:

I. Description of the Internet

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. Students and teachers have access to:

- Information and news from all over the world.
- Electronic mail communication.
- Copyrighted software as well as public domain and shareware of all types.
- Discussion groups on a variety of topics ranging from Chinese culture to the environment to music to politics.
- Library catalogs, the Library of Congress, ERIC, and other research institutions.
- Educational applications

II. Administration of the Network

The Superintendent of Schools shall designate an individual(s) to oversee the local area network (LAN) and the Internet connection. The individual(s) and/or his/her designee(s) shall:

- Monitor and examine network activities as appropriate to ensure proper use of the system.
- Be responsible for disseminating and interpreting district policy and regulations governing use of the district's network at the building level with all users.
- Coordinate employee training for proper use of the network resources and ensure that staff supervising students using these resources provide similar training to their students, including providing copies of district policy and regulations governing use of the district's network.
- Update the precautions to control Internet/network access as needed.
- Ensure that all media loaded onto the network have been scanned for computer viruses.

III. Network Use

- Internet/network access from school computers and other internet connected devices (ICD) is reserved solely for educational purposes. The District reserves the right to prioritize use and access to the system. The network users are advised that files that have not been read or modified within a certain period may be deleted.
- Users may access computers and ICD's only when staff who have had site-specific training by the District are available. Any use of the system must be in conformity to state and federal law and District policy. Use of the system for commercial solicitation is prohibited. Illegal activities are strictly forbidden.
- The system is a school district resource and may not be used to support or oppose political candidates or propositions submitted for vote to the electorate.
- No staff or student's use of the system shall disrupt the operation of the system by others; system components including, but not limited to hardware or software shall not be destroyed, modified, or abused in any way.
- Use of the system to develop or use programs to harass, intimidate others or to gain unauthorized access to any computer or computing system and/or damage the components of a computer or computing system is prohibited.
- Users are responsible for the appropriateness and content of material they transmit or publish on the system. Hate mail, harassment, discriminatory remarks, transmissions intended to embarrass others or disrupt the educational environment, or other antisocial or harmful behaviors are expressly prohibited.
- Use of the system to access, transmit, store, or distribute inappropriate, obscene or pornographic material or material of sexual content is prohibited.

- The unauthorized installation, use, storage, or distribution of copyrighted software, applications or any other materials on District computers or ICD's is prohibited. Users shall submit all storage media, including but not limited to diskettes, flash drives and cds to the site coordinator before they are placed in workstations.
- Any user of computer resources identified as a security risk or having a history of violations of district computer use guidelines may be denied access to the district's network/computer resources and could be subject to disciplinary measures.
- Staff members may use personal laptops or other electronic devices brought in from home to connect wirelessly to the district network only if a secure, wireless Virtual Local Area Network (VLAN) has been established in that school. Staff members using personal laptops or other electronic devices in this manner must sign a "Wireless VLAN Authorization Form" (4526-E), agree to the terms, conditions, responsibilities, and liabilities for such use, and abide by this and other district policies as well as applicable local, state and federal laws.
- Adult visitors and community members invited to the Hicksville Public Schools to conduct business, take adult education courses, or participate in evening, technology-based school events may use district equipment with guest network privileges (wireless network guest access). Requests for exceptions to this rule will be considered by the Director of Technology on a case-by-case basis. If an exception is granted, a temporary password will be made available for access to a guest-only wireless network.

The District retains the right to view and monitor any and all use of the system, including, but not limited to use of school computers, ICD's**,** internet/network use and e-mail by any person, including, but not limited to all students, staff and parents accessing and/or utilizing the system. Internet/network users have no expectation of privacy for activity, messages, e-mail, files or any usage of the District's network, Internet and/or system. Viewing or monitoring the use of the system, including, but not limited to school computers, ICD's, internet/network use and e-mail will only be done with the authorization of the Superintendent of Schools. Access to view the system or e-mails will be requested by any administrator and approved by the Superintendent of Schools. Access requested by the Superintendent of Schools will be approved by the Board of Education President or Vice President. The Board of Education will be notified of any viewing of district files or e-mails authorized by the Superintendent in an appropriate time and manner according to the reason for viewing the files or e-mails.

The electronic information available to students and staff does not imply endorsement of the content by the District, nor does the district guarantee the accuracy of information received on the Internet and use of information so obtained is at the user's own risk. 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 network use and to monitor file server space utilization by district users, while respecting the privacy rights of both district users and outside users. The Board establishes that use of the Internet and ICD applications is a privilege, not a right: inappropriate, unauthorized and illegal use will result in the cancellation of those privileges and appropriate disciplinary action.

IV. Privileges and Responsibilities

The use of the network is a privilege, not a right, and inappropriate use will result in a cancellation of that privilege. The user has the full responsibility for his/her account and, under no conditions, should the user share his/her account or password with any other person. The user shall not attempt to gain access to the computer under any name or password other than the one provided to him/her by the district.

V. Network Etiquette

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

1. Be polite. Inappropriate language and profanity are prohibited.
2. Do not reveal your social security number, personal address, phone number or credit card number, or those of other students or colleagues.
3. The impersonation of another user, anonymity, and pseudonyms are prohibited.
4. Electronic mail (e-mail) or other materials created by the user are not private. All new materials on the system, including, but not limited to e-mail, are subject to view by designated District officials.

VI. Notification Concerning Controversial Materials on the Internet/network

Each user of the computer network resources of the district has a responsibility to report controversial materials to the site coordinator in the event they are discovered on the user's workstation or ICD. Controversial material include materials that: 1) promote violence or advocate destruction of property including, but not limited to, access to information concerning the manufacture of destructive devices such as explosives, fireworks, smoke bombs, incendiary devices of the like; 2) promote pornography or other sexually oriented material; 3) advocate or promote violence or hatred against particular individuals or groups of individuals or advocate or promote the superiority of one racial, ethnic, or religious group over another; and 4) advocate and promote violence, or drug or alcohol use. These materials may be, but are not limited, to the following:

- Web site contents

- Viewable graphic files
- Text images
- Text documents containing controversial material
- Digitally encoded sound files
- Executable applications
- Printed material created by any of the above

VII. Consequences of Violations: The consequences for violating this policy will be consistent with other District policies and may include the following:
1. Notification of school authorities.
2. Notification of parent/guardian.
3. Suspension of access to the computer network and the Internet.
4. School consequences consistent with Policy 5300 Code of Conduct.
5. Financial restitution.
6. Legal action.

VIII. Responsibility with Respect to Created Materials

The site coordinator has the right to delete, read, or take other appropriate action with regard to controversial materials reported or discovered on the user's workstation, district server, or other ICD. The Hicksville Public School District extends the privilege of computer and ICD access for educational uses only. Users have no expectation of privacy for any materials created, copied, downloaded, or accessed by the user on the workstation or ICD including hard copies of such materials.

IX. The Hicksville Public School District makes no guarantees of any kind for the quality of service provided, nor shall the District be responsible for any service interruptions or the loss of, damage to, or the delay or unavailability, nondelivery or misdelivery of information when using the network, whether caused by its own negligence of the user's error or omissions.

X. Commercial Services

Subscriptions to mailing lists, bulletin boards, chat groups, applications and commercial online services, and other information must be pre-approved by the Hicksville Public School District. In addition to possible disciplinary action and loss of privileges, costs incurred for the unauthorized use of commercial services will be borne by the student, or for those under 18, the parent/guardian.

XI. Security Issues

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. Employees and students shall not reveal their passwords to another individual, other than a District official, so authorized to receive such information.

Users are not to use a computer that has been logged in another student's or employee's name.

Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the network or ICD, you must notify a K-12 administrator. Attempts to log on to the computer network as a system administrator or under a user name other than the one provided to the user will result in cancellation of user privileges and/or disciplinary action.

With the use of web-based programs, access is available via any computer or ICD with Internet capabilities. Employees with authorized access to these programs will maintain a private password in order to facilitate such access and take necessary precautions to ensure the security of student information.

XII. Vandalism will result in cancellation of district computer privileges and/or disciplinary action. This includes, but is in no way limited to the intentional uploading, creation and/or sending of computer viruses.

XII. Electronic mail is provided by the District to conduct business. All electronic messages created and stored on School District Computers or networks are property of the District and are not considered private. The District retains the right to access electronic mail and the District reserves the right to review all e-mail communication. Messages may be retrieved by the District even though the sender and reader have deleted them.

Accessing or reviewing e-mail communications will only be done with the authorization of the Superintendent of Schools. Access to view e-mails will be requested by any administrator and approved by the Superintendent of Schools. Access requested by the Superintendent of Schools will be approved by the Board of Education President or Vice President. The Board of Education will be notified of any viewing of e-mails authorized by the Superintendent of Schools in an appropriate timeframe and manner depending on the reason for viewing the files or e-mails.

District e-mail shall be used for work-related purposes only. The staff members with District e-mail shall use District e-mail, rather than personal e-mail, to correspond with any and all persons regarding work-related matters.

Board Approval Date:	January 23, 2002
Revised:	February 16, 2011
Reviewed:	April 17, 2013
Revised:	October 22, 2014
Revised:	August 30, 2015