SUBJECT: **COMPUTER NETWORK AND INTERNET SAFETY AND USE GUIDELINES**

In accordance with the authority provided by the Board of Education, the Plainview-Old Bethpage Central School District (the "District") establishes the following guidelines for implementing the District's Computer Network and Internet Safety and Use Policies:

I. General

1. The Superintendent of Schools shall designate a computer coordinator to oversee the District's computer network. The computer network coordinator shall monitor and examine all network activities, as appropriate, to ensure proper use of the system. The computer network coordinator shall be responsible for disseminating and interpreting District policy and guidelines governing use of the District's network at the building level with all network users. The computer network coordinator shall provide employee training for proper use of the network and will ensure that staff supervising students using the District's network provide similar training to their students, including providing copies of District policy and guidelines governing use of the District's network. The computer network coordinator shall ensure that all disks and software loaded onto the computer network have been scanned for computer viruses. All student agreements to abide by District policy and regulations and parental consent forms shall be distributed, managed, and kept on file in the building of the school attended by the student.

2. The District will monitor the online activities of minors through appropriate levels of administration and teachers. The District will provide appropriate guidance to students via the professional staff regarding what is lawful and what is appropriate usage of the District's online network systems.

3. The filtering system employed by the District will enable the District to restrict access to materials that are inappropriate and/or harmful to minors, as determined by the District. However, this system, while effective, is not foolproof and may from time to time provide access to inappropriate and/or harmful material. This filtering system, in conjunction with virus scanning software and firewall technologies, will also restrict access to Internet sites, hyperlinks, downloadable files, etc., that may potentially cause damage to the District's computer network. A user who incidentally connects to an inappropriate site must immediately disconnect from the site and notify a teacher or supervisor. If a user sees another user accessing inappropriate sites, he or she should notify a teacher or supervisor immediately.

4. Students and staff may not disable the District's filtering software at any time when students are using the Internet system if such disabling will cease to protect against access to inappropriate materials and Internet sites, hyperlinks, and/or files that can potentially damage the District's computer network. Authorized staff may temporarily or permanently unblock access to sites containing appropriate material and if the filtering software has inappropriately blocked access to such sites.

SUBJECT: **COMPUTER NETWORK AND INTERNET SAFETY AND USE GUIDELINES (Cont'd)**

5. It is the responsibility of all users of the District's computer network to be familiar with and adhere to the District's Computer Network and Internet Safety and Use Guidelines. All users and recipients of computer network accounts must participate in training pertaining to the proper use of the network. Account users are responsible for the maintenance of their accounts.

6. If any user can identify a security problem on the District's computer network, equipment, data, software or hardware, or on the Internet, the user must immediately notify the Superintendent of Schools or his/her designee.

7. All student users must be familiar with and adhere to the District's Computer Network and Internet Safety and Use Guidelines. Students are required to promptly disclose to a teacher, building administrator or staff member any received message that is inappropriate or makes them feel uncomfortable.

8. All staff, including teachers must be familiar with and adhere to the District's Computer Network and Internet Safety and Use Guidelines. Teachers are responsible for selecting material that is relevant to the course objectives and appropriate to the age of the students. Teachers will preview and review all material and on-line sites which they require students to access in order to determine the appropriateness and relevance of such material and on-line sites. In addition, teachers will provide guidelines and lists of resources to assist their students in properly channeling research activities. Furthermore, teachers will assist their students in developing skills to ascertain the truthfulness of information, to distinguish fact from opinion and will educate and supervise their students in the proper and appropriate use of the District's network system. Teachers must immediately forward to the building principal any reports from a student regarding inappropriate or uncomfortable messages received by the student.

9. Any specific request by a parent/guardian that the District not allow their child to have Internet access on the District's computer network must be made in writing, signed and dated by the parents or guardian and delivered to the student's building principal. Parents or guardians must make separate written requests for each child that will be denied Internet access by the District.

10. Any allegation that a student has violated the District's Computer Network and Internet Safety and Use Policies and these Guidelines, will be handled in accordance with District policy, the District's Code of Student Conduct and in accordance with any applicable law, statute or regulation.

11. Any allegation that a teacher, administrator, staff member, other employee or any other person, whether or not an authorized user, has violated the District's Computer Network and Internet Safety and Use Policies and these Guidelines, shall be handled in accordance with law, District policy and/or governing Collective Bargaining Agreements, if any.

SUBJECT: **COMPUTER NETWORK AND INTERNET SAFETY AND USE GUIDELINES (Cont'd)**

12. In order to protect the safety of all users and in exchange for access to and use of the District's computer network, all users must sign Acknowledgement of Responsibility form to be developed by the Superintendent and his/her designee that are legally binding and indicate that the party signing those forms have read and understood its contents and have read and understood the District's Computer Network and Internet Safety and Use Policies and these Guidelines and agree to be bound by the terms and conditions set forth in these documents.

13. Users of the District's computer network should not expect, nor does the District guarantee, privacy for any use of the District's computers or its computer network(s). The District reserves the right to access and view any material stored on District equipment or any material used in conjunction with the District's computer network. The District may monitor all use of the District's computer network and the Internet. There is no expectation of privacy in any file, information, data, mail or material located on or in any District computer or computer network account. The District reserves the right to conduct, at any time and without notice, reviews of all computers and computer network accounts to determine adherence to District policies, regulations and guidelines, including but not limited to the District's Computer Network and Internet Safety and Use Policies and these Guidelines. The District reserves the right to inspect, at any time and without notice, the contents of any file, information, data, mail or material stored on or in its computers and its computer network(s).

14. Home and personal Internet use can have an impact on the school and on other students. If students' personal Internet expression-such as a threatening message to another student or a violent Web site-creates a likelihood of material disruption of the school's operations, students may face school discipline and criminal penalties.

II. **Internet Access**

1. Students:

Students may be provided access to the Internet during class time or during instruction time in a supervised environment.

Students may be provided with individual accounts.

Students will not have individual e-mail addresses sponsored by the District.

Students are not allowed to belong to mailing lists.

2. **Prohibited Uses**: The following is a list of prohibited uses of the District's computer network system, equipment, software and/or hardware:

SUBJECT: **COMPUTER NETWORK AND INTERNET SAFETY AND USE GUIDELINES (Cont'd)**

a. Downloading, uploading, accessing, distributing or displaying of any material, or any other use of the District's computer network, equipment, data, software and/or hardware, that violates any federal or state statute, law or regulation is prohibited. This prohibition includes but is not limited to material protected by copyright laws, threatening material, obscene or pornographic material, or material protected by trade secret;

b. Messages or other electronic data relating to or in support of illegal activities are prohibited and may be reported to the authorities or the Superintendent or his/her designee. The District will cooperate with local, state or federal officials in any investigation concerning or relating to any illegal activities conducted through the District's computer network system;

c. Use of the District's computer network, equipment, software and/or hardware for personal and/or commercial activity is prohibited, including but not limited to personal purchases;

d. Vandalism of any kind, through the use of computer viruses or by any other means, is prohibited. Vandalism includes but is not limited to intentionally and/or maliciously harming, damaging or destroying, or attempting to harm, damage or destroy, any portion of the District's computer network, equipment, data, software and/or hardware, intentionally and/or maliciously harming or destroying, or attempting to harm or destroy, any data stored on the District's computer network, intentionally and/or maliciously harming or destroying, or attempting to harm or destroy, any portion of any computer network, equipment, data, software, and/or hardware belonging to any other user or belonging to the Internet of belonging to any other agency, entity, person or network connected to the Internet. Any person who commits any act of vandalism to the District's computer network, equipment, data, software, and/or hardware will be fully responsible for all costs incurred by the District as a result of such vandalism, including but not limited to the costs related to the repair and/or replacement of any portion of the District's computer network, equipment, data, affected in any way by such act of vandalism;

e. Downloading, uploading, accessing, distributing or displaying material is prohibited that, in the opinion of the administration, is obscene or pornographic, offensive to others, abusive of another person or group of persons, advocating violence, denigrating to people based on gender, race, ethnicity, religious beliefs or sexual identity, promoting the use of alcohol, tobacco, drugs, hate or weapons;

f. Disclosing account passwords;

g. Using passwords belonging to other users, attempting to access another user's account and/or accessing another user's account and/or accessing another user's folders, work or files;

h. Sharing of passwords or accounts with any other person;

SUBJECT: **COMPUTER NETWORK AND INTERNET SAFETY AND USE GUIDELINES (Cont'd)**

i. Placing unauthorized software or hardware on District computers;

j. Downloading, uploading, accessing, transmitting or distributing viruses;

k. Intentionally wasting computer network, equipment, software and/or hardware resources;

l. Using the District's computer network, equipment, software and/or hardware for product advertisement or political lobbying;

m. Bypassing or disabling, or attempting to bypass or disable, the filtering technology and/or software employed by the District is prohibited. Notwithstanding the foregoing, however, an administrator, supervisor or other person authorized by the District may disable the filtering technology during use by an adult to enable access to the Internet for bona fide research or other lawful purpose consistent with the District's Internet Safety and Use Policies and these Guidelines;

n. Plagiarizing another's work is prohibited. District policies and procedures on plagiarism will govern the use of material accessed through the system. All users are to use appropriate research and citation practices;

o. Posting of personal identifying information belonging to oneself or any other person on websites; except that authorized District staff only may post directory information photographs of students on the District's website unless the parent or guardian or eligible student has informed the student's principal in writing by November 1st of the school year that he or she has opted out of or restricts access to or disclosure of directory information;

p. Revealing any personally identifying information belonging to oneself or any other person is prohibited, except that authorized District staff may post directory information photographs of students on the District's website unless the parent or guardian or eligible student has informed the student's principal in writing by November 1st of the school year that he or she has opted out of an restricts access to or disclosure of directory information;

q. Logging in to the District's computer network(s) or the Internet as "System Administrator," or attempting to do so;

r. The use of disrespectful, defamatory, inflammatory, obscene, vulgar, lewd, profane, rude, threatening, bigoted, harassing or illegal language or messages, cyber bullying;

s. Posting or transmitting of chain e-mail letters; and,

t. Cyber Bullying which is defined as the use of electronic information and communication devices such as e-mail, instant messaging, text messaging, mobile phones, pagers and defamatory websites to bully or otherwise harass an individual or group through personal attacks or other means.

SUBJECT: **COMPUTER NETWORK AND INTERNET SAFETY AND USE GUIDELINES (Cont'd)**

3. **Netiquette**: While online or accessing the Internet, all persons are expected to abide by the generally accepted rules of network etiquette, including but not limited to the following:

a. All users must be polite at all times;
b. Only appropriate language may be used in communications, messages and transmissions;
c. The District's computer network shall not be used in any way that disrupts its use by others;

d. Use of the system and the data acquired must be in strict compliance with law; and

e. Receiving, sending, or forwarding another person's messages without that person's authorization should be avoided.

4. **Electronic mail, chat rooms, and other forms of direct electronic communications (i.e. instant messaging services):** Students may not access "chat rooms" or utilize direct electronic communications, i.e. instant messaging services, via the District's computer network except when limited permission is granted in cases where such access is necessary for education or research and is technically feasible within the context of providing adequate security. Other users of the District's computer network may only access chat rooms and direct electronic communications for purposes that are consistent with the educational objectives of the District or for work productivity. In all cases such access must be in compliance with the District's Computer Network and Internet Safety and Use Policies and these Guidelines.

5. **Disclaimer and Limitation of Liability:** The District makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the District's computer network system will be error-free or without defect. The District is not responsible for any damages users may suffer, including but not limited to, loss of data resulting from delays, non-deliveries, error or omissions, or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. It is the responsibility of each user to verify the integrity and authenticity of the information that is used. The use of any information

obtained via the Internet is at the user's own risk. The District is not responsible for financial obligations arising through the use of the system, unless expressly authorized by the District's Board of Education.

Reservation of Rights: The District reserves the right and discretion to modify and/or amend these District's Computer Network and Internet Safety and Use Policies and these Guidelines.

Authorized: 11/15/04
Updated: 10/06/06
Updated w/changes: 6/20/11