SUBJECT: **INTERNET SAFETY AND USE POLICIES**

The Plainview-Old Bethpage Central School District (the "District") supports the usage of the District's computer network by students and employees in order to access the Internet for purposes consistent with the educational goals of the District and District policies. Internet access is available to students, administrators, teachers and staff as part of a collaborative instructional project between the District and a service provider. The network may be accessed by authorized users of the District's network who have signed and submitted the District's Summary and Consent forms. In addition to access to the District's computer network through the District's computers and/or District issued/owned mobile devices, the network may also be accessed through the use of personal mobile devices such as tablets, smart phones, and laptop computers in the areas specifically designated by the District for personal mobile device access.

With the advent of web/cloud-based network instructional activities that require the District to set up individual student and staff user accounts, the minimum required personal information will be provided to third party District approved hosts/service providers solely for the purpose of accessing such services in alignment with the District's Parents' Bill of Rights for Data Privacy and Security, Children's Online Privacy Protection Act (COPPA), http://www.ftc.gov/privacy/coppafaqs.shtm and the Children's Internet Protection Act (CIPA) https://www.fcc.gov/consumers/guides/childrens-internet-protection-act. Unless a parent/guardian denies such access for their child via formal written request, the District will be permitted to set up such accounts, including Google Apps for Education, for example, to provide students and staff with the appropriate access they may require. The act of signing the Internet Safety and Use policy agreement provides consent for the district to create user accounts from District approved third party cloud-based providers.

All access to the District's computer network and all use of the District's computer network must be for purposes consistent with the educational goals of the District and must be in strict compliance with all District policies and regulations including but not limited to the District's Internet Safety and Use Policies and Guidelines, the Code of Conduct, and the District's Anti-Bullying and Harassment Policy (No. 7580). The District's goal in providing access to its computer network is to promote educational excellence by facilitating resource sharing, innovation, and system communication. In order to ensure user safety and the integrity of the networked system, and in order to comply with federal regulations requiring Internet filtering for schools and libraries receiving E-Rate and Title III funds, the District adopts the following Internet Safety and Use Policy and Guidelines:

(Continued)

Internet Filtering Services:

The District will employ filtering technology on all District computers with Internet access and on its computer network and will monitor the online activities of minors and adults on District computers and on the District's computer network. Please note, the District's filtering system and monitoring of online activities will be applicable to all users of the District's computer network whether access to the Internet is on a District computer, a District issued/owned mobile device or a personal mobile device. The filtering system employed by the District will enable the District to operate technology protection measures that will block and/or filter access by minors and adults to depictions on the Internet that are:

a. Obscene;
b. pornographic;
c. harmful to minors

This filtering system will also enable the District to restrict access to materials that are inappropriate and/or harmful to minors. However, this filtering system, while effective, is not foolproof and may from time to time provide access to inappropriate and/or harmful material.

The District will maintain firewall technology on its computer network to ensure that student information is not publicly accessible to unauthorized users, and the District professional staff will provide guidance, instruction and supervision to students in order to educate them regarding the importance of Internet privacy and anonymity.

Responsibilities of All Users:

It is the responsibility of all users of the District's computer network to be familiar with and adhere to the District's Internet Safety and Use Policies and accompanying Guidelines.

Parent/Guardian Responsibility for Safe Internet Use by Students

The Internet Safety and Use Policies and accompanying Guidelines are available for review by parents or guardians on request and are posted on the District's website. Parents or guardians should be familiar with them.

The Internet Safety and Use Policies and accompanying Guidelines contain restrictions on accessing inappropriate and/or harmful material on the Internet through the District's computer network in order to protect users. In addition, the District will employ filtering technology and will monitor and attempt to properly channel on-line activities of students. However, there is a wide range of material available on the Internet that may not be in keeping with the particular views of the families of the students. The District recognizes that parents have primary responsibility for transmitting their particular set of values to their children and that the parents or guardians of minors are ultimately responsible for setting and conveying standards that their children should follow when using the Internet, media and information sources. Parents are also responsible for monitoring the students' use of the Internet and the District's network if students are using the District's computer network to access the Internet from home.

The District believes that the benefits to students of Internet access that result from the vast amount of information resources and opportunities for collaboration outweigh the disadvantages of such access.

Privileges of Internet Access and Penalties and Procedures for Violations:
In order to protect the safety of all users of the District's computer network(s), the District's computer network(s) is to be used for educational and work productivity purposes that are consistent with the goals of the District and in strict compliance with all District policies and regulations. 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.

Use of the network(s) is a privilege, not a right. The District reserves the right to determine who may have access to its network(s). Any user identified as a security risk or who has a history of inappropriate Internet use or a history of inappropriate use of the District's computer network(s) or the computer network of any other agency or entity may be denied access to the District's computer network(s) and the Internet.

There is no expectation of privacy in any file, information, data, mail or material located on or in any District computer, District issued/owned mobile device or computer network account and there is no expectation of privacy in any District computer, District issued/owned mobile device.

The District reserves the right to conduct, at any time and without notice, reviews of all computers, District issued/owned mobile devices and computer network accounts to determine adherence to the District's Internet Safety and Use Policies and accompanying Guidelines. The District reserves the right to inspect, at any time and without notice, the

(Continued)

contents of any file, information, data, mail or material stored on or in its computers and its computer network(s).

Inappropriate use and any violation of the Internet Use Policies and accompanying Guidelines or any District policy or regulation by any user, including students, teachers, administrators and staff, may result in the loss of network privileges or other disciplinary action as deemed appropriate by the Board of Education, the Superintendent of Schools, the building principal or their designee.

The Superintendent and/or his/her designee are authorized to enact the Guidelines to accompany and implement the District's Internet Safety and Use Policies.

DISTRICT INTERNET USE POLICY

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. With electronic access to the Internet through computers and mobile devices, to people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. The smooth operation of the network relies upon the proper conduct of the end user who must adhere to the following and to the District's Guidelines that are provided so that users are aware of the responsibilities they are about to acquire:

Purpose of Internet Access: All users, including students, teachers, administrators and staff, are responsible for their behavior and communications over the District's computer network. The use of the District's computer network(s) for access to the Internet and the use of a District account must be in support of education, research or work productivity and must be consistent with the educational objectives of the District and all District policies including but not limited to the Code of Conduct and the District's Anti-Bullying and Harassment Policy (No. 7580). Students, teachers, administrators and staff shall have Internet access in order to:

a. Communicate with people all over the world;
b. Access information and news from various governmental agencies and research institutions;
c. Access university library catalogs, the Library of Congress, etc.;
d. Conduct District business

Student Access: Students may have access to the Internet through the District's computer network. Students' use of the network will be governed by the District's policies, regulations and guidelines including but not limited to the District's Internet Safety and Use Policies, by the accompanying Guidelines established by the District, by the District's Student Code of Conduct, Field Trip Policy, Anti-Bullying and Harassment Policy (No. 7580) and by the

District's discipline policy. Students are responsible for good behavior on the District's computer network just as they are in a classroom or a school hallway.

Use of Other Networks: Use of another organization's network or computing resources through District equipment, software or hardware must comply with the rules of that network and with the District's Internet Safety and Use Policies and accompanying Guidelines and with all District policies.

Use of District Computer Network: The Superintendent and/or his/her designee shall establish Guidelines that will serve as the rules and regulations governing the use of the District's computers and its computer network(s). Students will be provided with guidance regarding what is lawful and what is appropriate usage of the District's network systems.

Netiquette: While online or accessing the Internet, all persons are expected to abide by the generally accepted rules of network etiquette.

Monitored Use: All files, information, data, mail or material, including but not limited to, communications, messages and transmissions, that use the District's computer network, equipment, data, software and/or hardware should be assumed to be and are the property of the District and users shall not have any expectation of privacy in such files, information, data, mail or material. Electronic mail transmissions and other electronic communication system(s) by any user of the District's computer network, equipment, data, software and/or hardware shall not be considered and are not confidential and may be monitored at any time by designated staff to ensure appropriate use for educational or work productivity purposes.

Note that all electronic mail (e-mail) and data files are not private and must be consistent with the educational objectives of the District, all District policies and/or work productivity. People who operate the District's computer network systems have access to all files, information, data, mail or material on the District's computers, District issued/owned mobile devices and/or the District's computer network system(s).

Moreover, routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the District's Internet Safety and Use Policies and accompanying Guidelines, other District policies or the law. Searches will be conducted if there is suspicion that a user has violated the District's policies, regulations and guidelines including but not limited to the District's Internet Safety and Use Policies and accompanying Guidelines, other District policies or the law.

(Continued)

Disclaimer and Limitation of Liability: The District is not responsible for any misuse of the privileges granted hereunder or any misuse of its computer network(s), equipment, software and/or hardware. Users agree to indemnify the District and hold it harmless in accordance with the terms set forth in the Acknowledgment of Responsibilities form signed by the user and parent or guardian where the user is a student.

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(s) 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 District's computer network system, unless expressly authorized by the District's Board of Education.

Resource Limits: The District reserves the right to set maximum size limits for hard disk memory and other usage on the District computer systems. Users who are in noncompliance with quotas will have their files removed or access limited by a system administrator. The Building Principal or his/her designee has the authority to limit use of the District's computer network system. Files, information, data, mail or material stored or saved by students or staff on or in the District's computers, District issued/owned mobile devices or computer network systems are subject to removal by the District. Users are urged to make copies of documents they wish to preserve. The District makes no guarantee that files, information, data, mail or material will not be erased or destroyed by any means at any time.

The Board of Education authorizes the Superintendent of Schools and/or his/her designee to establish the Guidelines to accompany and implement the District's Internet Safety and Use Policies set forth herein.

Under Review: 4/7/04
Adopted: 11/15/04
Amended w/changes: 3/11/13
Circulate with changes: 6/9/16
Amended with changes: 8/10/16

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 network 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 Policies and these 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 Policies and 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 Policies and 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. Teacher directed internet activities are part of our curriculum and not subject to parent/guardian authorization and/or consent.

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

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. In order to access the district's computer network, all users must have on file with the district a fully completed and signed consent form or user agreement, as applicable.

Consequences of Violations 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 the Code of Conduct.
5. Financial restitution.
6. Legal action.

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. In order to access the district's computer network, all users must have on file with the district a fully completed and signed consent form or user agreement, as applicable.

Consequences of Violations may include the following:
1. Notification of school authorities.
2. Suspension of access to the computer network and the Internet.
3. School consequences consistent with the Code of Conduct.
4. Financial restitution.
5. Legal action.

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 forms to be developed by the Superintendent or 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 such Policies and Guidelines.

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, any District issued/owned equipment including but not limited to mobile devices or its computer network(s). The District reserves the right to access and view any material stored on District equipment or

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

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, any District owned/issued equipment including but not limited to mobile devices, 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 all District policies, regulations and guidelines, including but not limited to the District's Computer Network and Internet Safety and Use Policies, these Guidelines, the District's Code of Conduct and the District's Anti-Bullying and Harassment Policy (No. 7580). 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:

Mobile devices with access to the Internet are becoming the norm. For today's students, in this highly connected, information intensive world, learning is a 24/7 enterprise and the traditional school day is only a small segment of their learning day. These changes in technology necessitate a similar change in policy. Students may be provided access to the Internet during class time or during instruction time environment or in any area designated by the District for internet access on personal mobile devices.

Students may be provided with individual accounts.

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

Unless specifically approved in advance and use for education purposes, students are not allowed to belong to mailing lists through the District's computer network.

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

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;

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, including but not limited to excessive use of band width;

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

m. Bypassing or disabling, hacking 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 personally identifying information belonging to oneself or any other person on web sites;

p. Revealing any personally identifying information belonging to oneself or any other person is prohibited. Such information includes but is not limited to last name, social security number, home address, telephone number and credit card numbers;

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, discriminatory, harassing or illegal language or messages;

s. Cyberbullying;

t. Engaging in any act or conduct that violates any District Policy, including but not limited to the District's Code of Conduct and the District's Anti-Bullying and Harassment Policy (No. 7580); and

u. Posting or transmitting of chain e-mail letter.

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):** The Board of Education acknowledges that the "spirit" of computer networks is to foster collaboration and communication. However, monitoring is necessary to ensure that collaboration and communication occurs in a safe and secure environment. Unless specifically approved in advance and used for educational purposes, 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 and all District Policies including but not limited to the District's Code of Conduct and the District's Anti-Bullying and Harassment Policy (No. 7580).

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.

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

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
Amended w/changes: 3/11/13