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)

3

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