INTERNET SAFETY

The Bellmore-Merrick Central High School District is committed to undertaking efforts that will serve to make the use of district computers for access to the Internet and digital platforms safe for our children. To this end, although unable to guarantee that any customized filtering and blocking technology will work perfectly, the Board of Education directs the Superintendent of Schools to procure and implement the use of technology protection measures that block or filter Internet access by:

- adults to visual depictions that are obscene or pornography, especially child pornography, and
- minors to visual depictions that are obscene, pornography especially child pornography, or harmful to minors.

Upon the submission of a written request for access to certain websites and with the Director of Administrative and Instructional Technology, any such measures may be disabled or relaxed for adults conducting bona fide research or other lawful purposes, in accordance with criteria established by the Superintendent or his or her designee.

The Superintendent or his or her designee also shall develop and implement procedures that provide for the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of students using district computers; and restricting student access to materials that are harmful to minors including that promote violent or aggressive acts.

In addition, the Board prohibits the unauthorized disclosure, use and dissemination of personal information regarding students; unauthorized online access by students, including hacking, and other unlawful activities; and access by students to inappropriate matter on the Internet. The Superintendent or his or her designee shall establish and implement procedures that enforce these restrictions.

The Director of Administrative and Instructional Technology and his or her designee designated under the district's Computer Network or Acceptable Use Policy, shall monitor and examine all district computer network activities to ensure compliance with this policy and accompanying regulation. He or she also shall be responsible for ensuring that staff and students receive training and or notification on their requirements.

Adopted: 09/04/2019
2nd Reading (Revised): 09/04/2019
1st Reading (Revised): 08/07/2019
Adopted: 08/01/2012
2nd Reading (Revised): 08/01/2012
1st Reading (Revised): 07/10/2012
Adopted: 01/06/2010
2nd reading: 01/06/2010
1st reading: 02/02/2009

Harassment – Students are prohibited from posting on digital platforms harassing texts or images, which include, but are not limited to, those that defame, degrade, discriminate**,** threaten are abusive, intimidate or falsely accuse another individual of wrongdoing or illegal behavior. This includes, but is not limited to, such social networking sites as Facebook, YouTube, Twitter, etc.

All users of the district's computer network, including access to the Internet, must understand that use is a privilege, not a right, and that any such use entails responsibility. When using the network the individual will respect and protect the privacy of others. Passwords will not be shared or stolen. They must comply with the requirements of this policy and accompanying regulation, in addition to generally accepted rules of network etiquette, and the district's Terms and Conditions for use of Network and Internet Services in the Bellmore-Merrick CHSD. Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges.

In order to provide for the education of all users, minors and adults, regarding appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms and any other web format and cyber bullying awareness and response, all students will complete a unit of study on this topic in the 7th grade technology class. In addition, the Assistant Superintendent for Personnel & Administration provides training for all employees annually.

Ref: Public Law No. 106-554
47 USC §254
20 USC §6777
47 CFR §54.520

INTERNET SAFETY REGULATION

The following rules and regulations implement the Internet Safety Policy adopted by the Board of Education to make safe for children the use of district computers for access to the Internet.

I. Definitions

In accordance with the Children's Internet Protection Act,

- *Child pornography* refers to any visual depiction, including any photograph, film, video, picture or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. It also includes any such visual depiction that (a) is a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct; or (b) has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
- *Harmful to minors* means any picture, image, graphic image file, or other visual depiction that (a) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (b) depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (c) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

II. Blocking and Filtering Measures

- The Superintendent or his or her designee shall secure information about, and ensure the purchase or provision of, technology protection measures that block access from all district computers to visual depictions on the Internet that are obscene, child pornography or harmful to minors.
- The district's Director of Administrative and Instructional Technology shall be responsible for ensuring the installation and proper use of any Internet blocking and filtering technology protection measures obtained by the district.
- The Director of Administrative and Instructional Technology may allow access to sites on the Internet that are blocked by the District filter only for adult staff members or students conducting research related to the discharge of their official responsibilities. A request by a staff member must be made in writing that includes the website address for review, reason why the access is needed, and specific length of time access will be needed.

- The Director of Administrative and Instructional Technology or his/her designee shall monitor the online activities of adult staff members or students for whom the blocking and filtering technology measures has been disabled or relaxed to ensure there is not access to visual depictions that are obscene or child pornography.

III. Monitoring of Online Activities

- Upon logging into the district network, users must acknowledge that he/she has read and agreed to terms of Computer Network or Acceptable Use Policy in the Bellmore-Merrick CHSD.
- The district's Director of Administrative and Instructional Technology shall be responsible for monitoring to ensure that the online activities of staff and students are consistent with the district's Internet Safety Policy and this regulation. He or she may inspect, copy, review, and store at any time, and without prior notice, any and all usage of the district's computer network for accessing the Internet and direct electronic communications, as well as any and all information transmitted or received during such use. All users of the district's computer network shall have no expectation of privacy regarding any such materials.
- It is expected that students and staff members respect the integrity and security of the network.
- Except as otherwise authorized under the district's Computer Network or Acceptable Use Policy, students may use the district's computer network to access the Internet only during supervised class time, study periods or at the school library, and exclusively for research related to their course work.
- Staff supervising students using district computers shall help to monitor student online activities to ensure students access the Internet, and/or participate in authorized forms of direct electronic communications in accordance with the district's Internet Safety Policy and this regulation.
- The district's Director of Administrative and Instructional Technology shall monitor student online activities to ensure students are not engaging in hacking (gaining or attempting to gain unauthorized access to other computers or computer systems), and other unlawful activities.
- Personal use is restricted. The District prohibits the use of network computers for conducting personal business.
- Virtual Private Networks – Students and staff are prohibited from using virtual private networks, proxies, and/or other methods used to circumvent the district network security measures.

IV. *Training*

- The district's Director of Administrative and Instructional Technology shall provide training and or notification to staff and students on the requirements of the Internet Safety Policy and this regulation at the beginning of each school year.
- The training of staff and students shall highlight the various activities prohibited by the Internet Safety Policy, and the responsibility of staff to monitor student online activities to ensure compliance therewith.

- Students shall be directed to consult with their classroom teacher if they are unsure whether their contemplated activities when accessing the Internet are directly related to their course work.
- Staff and students will be advised to not disclose, use and disseminate personal information about students when accessing the Internet or engaging in authorized forms of direct electronic communications.
- The district will provide education to all users, minors and adults, regarding appropriate online behavior, including interacting with other individuals on social network websites and in chat rooms and any other web format and cyber bullying awareness and response. Such education shall be provided to students as a unit of study in the 7th grade technology class. In addition, the Assistant Superintendent for Personnel provides training for all employees annually.
- Staff and students will also be informed of the range of possible consequences attendant to a violation of the Internet Safety Policy and this regulation.

V. *Reporting of Violations*

- Violations of the Internet Safety Policy and this regulation by students and staff shall be reported to the Building Principal. The principal will communicate incidents to the Director of Administrative and Instructional Technology.
- The Principal shall take appropriate corrective action in accordance with authorized disciplinary procedures.
- Penalties may include, but are not limited to, the revocation of computer access privileges, as well as school suspension in the case of students and disciplinary charges in the case of staff members.