COMPUTER USE and INTERNET SAFETY REGULATION

The following rules and regulations shall govern the implementation of the Internet Safety Policy adopted by the Board of Education to create a safe Internet environment for the school community.

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, or appears to be, 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; or (c) is advertised, promoted, presented, described, or distributed in such a manner than conveys the impression that the material is or contains a visual depiction of a minor 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.

- *Social Media* has become a useful communication and collaboration tool and may be used responsibly for educational and promotional purposes. Social media includes all online interaction methods including but not limited to blogs, Office 365's Yammer, O365 Tools, and other social network sites. The Dignity for All Students Act and the District's Code of Conduct prohibit all forms of bullying (including Cyberbullying) and outline the District's responsibility to address incidents that take place in the District and outside the District that could disrupt the school environment.

II. Blocking and Filtering Measures

- The Superintendent or his or her designee shall procure and implement technology protection measures that block or filter access to the Internet appropriately
- The District's Assistant Superintendent for Technology shall be responsible for ensuring the installation and proper use of any Internet blocking and filtering technology protection measure obtained by the District.
- The Assistant Superintendent for Technology or his or her designee may disable or modify the District's Internet blocking and filtering technology measure only for

adult staff members conducting research related to the discharge of their official responsibilities.

- The Assistant Superintendent for Technology or his or her designee shall monitor the online activities of adult staff members for whom the blocking and filtering technology measure has been disabled or modified to ensure there is not access to visual depictions that are obscene or child pornography.

III. Monitoring of Online Activities

- The District's Assistant Superintendent for 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.
- Students may use the District's computer network to access the Internet only in accordance with regulations outlined in the Acceptable Use Policy, the Code of Conduct, the Student and Personal Electronic Devices Policy, and building handbooks.
- Staff supervising students using electronic devices 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 this regulation and the District's Internet Safety Policy.
- The District's Assistant Superintendent for 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.

IV. Training

- The District's Assistant Superintendent for Technology shall provide training to staff and students on the requirements of the Computer Use and 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 Computer Use and Computer Use and Internet Safety Policy, and the responsibility of staff to monitor student online activities to ensure compliance therewith.
- The District shall provide age-appropriate instruction to students regarding appropriate online behavior. Such instruction shall include but not be limited to: appropriate interactions with others online; protection from online predators; personal safety when using the Internet; and how to recognize and respond to cyberbullying and other threats.

COMPUTER USE and INTERNET SAFETY REGULATION

- 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 or disseminate personal information about students when accessing the Internet or engaging in authorized forms of direct electronic communications.
- Staff and students will also be informed of the range of possible consequences attendant to a violation of the Computer Use and 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 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 teachers.

Cross Ref:
District Code of Conduct
Dignity for All Students Act, Education Law §801-a; Education Law, Article 2
5695 Students and Personal Electronic Devices

Board Adoption Date: February 15, 2018