VALLEY STREAM UNION FREE SCHOOL DISTRICT TWENTY FOUR

INTERNET SAFETY **Policy 6167**

The Superintendent of Schools, or his or her designee, 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 School District computers; and restricting student access to materials that are harmful to minors as defined in the Children's Internet Protection Act.

The Board of Education is committed to undertaking efforts that serve to make safe for children the use of School District computer resources, e.g. computers, computer systems, computer software/applications, and/or computer networks, including the internet (hereinafter the "School District's computer resources") for access to the Internet and World Wide Web. To this end, although unable to guarantee that any selected filtering and blocking technology will work perfectly, the Board of Education directs the Superintendent of Schools or his/her designee 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 child pornography; and
- minors to visual depictions that are obscene, child pornography, or harmful to minors, as defined in the Children's Internet Protection Act.

Subject to staff supervision, however, any such measures may be overridden for conducting bona fide student research or other lawful purposes, in accordance with criteria established by the Superintendent of Schools or his /her designee.

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.

Blocking and Filtering Measures

- The Superintendent of Schools or his/her designee shall secure information about, and direct the purchase or provision of, a technology protection measure that blocks access from all School District computer resources to visual depictions on the Internet and World Wide Web that are obscene, child pornography or harmful to minors.

- The Superintendent of Schools or his/her designee shall be responsible for ensuring the installation and proper use of any Internet blocking and filtering technology protection measure obtained by the School District.

- The Superintendent of Schools or his/her designee may disable or relax the School District's Internet blocking and filtering technology measure only for adult staff members conducting research related to the discharge of their official responsibilities.

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

Monitoring of Online Activities

- The Superintendent of Schools or his/her designee shall be responsible for monitoring to determine that the online activities of staff and students are consistent with this policy. He/She may inspect, copy, review, and store at any time, and without prior notice, any and all usage of the School District's computer resources for accessing the Internet and World Wide Web and direct electronic communications, as well as any and all information transmitted or received during such use. All users of the School District's computer resources shall have no expectation of privacy regarding any such materials.

- Except as otherwise authorized under Policy 6166 (Computer, Network and Internet Acceptable Use), students may use the School District's computer resources to access the Internet and World Wide Web 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 School District computer resources shall help to monitor student online activities to determine the appropriateness of student access to the Internet and World Wide Web, and/or authorized forms of direct electronic communications in accordance with this policy.

- The Superintendent of Schools or his/her designee shall monitor student online activities to ascertain whether students are engaging in hacking (gaining or attempting

to gain unauthorized access to other computers, or computer resources), and other unlawful activities.

Training

- The Superintendent of Schools or his/her designee shall provide training to staff and students on the requirements of this policy at the beginning of each school year.

- The training of staff and students shall highlight the various activities prohibited by this policy and the responsibility of staff to monitor student online activities to determine compliance therewith.

- The School District shall provide age-appropriate instruction to students regarding appropriate online behavior. Such instruction shall include, but not be limited to: positive interactions with others online, including on social networking sites and in chat rooms; proper online social etiquette; protection from online predators and personal safety; and how to recognize and respond to cyberbullying and other threats.

- Students shall be directed to consult with their classroom teacher if they are unsure whether their contemplated activities requiring the use of 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.

Violations

- Violations of this policy by students and staff shall be reported to the Building Principal.

- The Principal shall take appropriate corrective action in accordance with the School District's Code of Conduct.

- 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.

In addition, the Board of Education 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 and World Wide Web. The Superintendent of Schools, or his or her designee, shall establish and implement procedures that enforce these restrictions.

All users of the School District's computer resources, including access to the Internet and World Wide Web, must understand that use is a privilege, not a right, and that any such use entails

responsibility. They must comply with the requirements of this policy, in addition to generally accepted rules of network etiquette, and the School District's policy on the acceptable use of computer resources.

Cross-ref: 0115 Dignity for All Students Act
5131 Code of Conduct
6165 Computer Resources and Data Management
6166 Computer, Network and Internet Acceptable Use
6168 Information Security Breach and Notification

Ref: Children's Internet Protection Act, Public Law No. 106-554
Broadband Data Services Improvement Act/ Protecting Children in the 21st Century Act, Public Law No. 110-385
47 USC §254
20 USC §6777

Adoption Date: June 12, 2019