(X) Required
( ) Local
(X) Notice

INTERNET SAFETY POLICY

The Board of Education is committed to providing safe access to the Internet in the use of District computers and other technology. To this end, although unable to guarantee that any selected filtering and blocking technology will work perfectly, the Board authorizes the Superintendent of Schools to develop, disseminate, and implement regulations and procedures inclusive of technology protection measures that block or filter Internet access by:

- adults and minors to visual depictions that are obscene, child pornography, or harmful to minors, as defined in the Children's Internet Protection Act.

Any such measures may be disabled or relaxed for adults conducting or supervising *bona fide* research or for other lawful purposes. Teachers or administrators may request access to a restricted site. Subject to staff supervision, technology protection measures may be disabled, or, in the case of minors, minimized only for *bona fide* research or for other lawful purposes. However, the law does not require that a school district afford adults unfiltered access to the Internet, even for a *bona fide* request.

The Superintendent of Schools or designee also shall develop and implement procedures that provide for the safety and security of students using digital and electronic mail, texting, social networks, chat boxes, and any/all forms of direct digital communications; monitor the online activities of students using district computers and district-provided accounts; and restrict student access to materials that are harmful to minors.

In addition, the Board prohibits the unauthorized disclosure, use, and dissemination of personal information regarding students and staff; unauthorized online access by users, including hacking and other unlawful activities; and access by users to inappropriate matters on the Internet. The Superintendent of Schools, or designee, shall establish and implement procedures that enforce these restrictions. The Superintendent of Schools, or designee, shall be responsible for ensuring that staff and students receive training on acceptable use.

The Superintendent, or designee, shall monitor and examine District technology activities to ensure compliance with this policy and accompanying regulations. Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent or designated representatives.

It shall be the responsibility of all Hewlett-Woodmere Public Schools staff to supervise and monitor the usage of District technology in accordance with this policy, the Children's Internet Protection Act (CIPA), and the Hewlett-Woodmere Schools Network and Internet Acceptable Use Policy, Policy No. 4526.

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. They must comply with the requirements of this policy and accompanying regulations, in addition to generally accepted rules of network etiquette, and the District's Acceptable Use Policy. Circumventing technology protection measures by connecting a District device to an unapproved internet source, such as a portable hotspot, smartphone tether, virtual private network (VPN), or any other device is prohibited. Failure to comply may result in an investigation, which could lead to the temporary modification or revocation of computer access privileges and/or disciplinary action. Attempting to bypass District filtering measures is strictly prohibited.

The following rules and regulations outline the specifications of the Internet Safety Policy adopted by the Board of Education to ensure the safety of children's 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 a photograph, film, video, picture of 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 what is suitable for 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 designee shall secure information about, and ensure the purchase or provision of technology protection measure(s) that block access from all District technology to visual depictions on the Internet and that are obscene, child pornography, and/or harmful to minors.
- The Superintendent or designee shall be responsible for ensuring the installation, proper configuration, and use of any Internet blocking and filtering technology protection measure obtained by the District as authorized.
- When authorized, the Superintendent or designee may disable or relax the District's Internet blocking and filtering technology measure only for adult staff members conducting *bona fide* research or for other lawful purposes related to the discharge of

their official responsibilities.

- When authorized, the Superintendent or designee shall monitor the online activities of adult staff members for whom the blocking and filtering technology measure has been disabled or relaxed to ensure there is no access to visual depictions that are obscene child pornography and/or harmful to minors.

III. Monitoring of Online Activities

- The Superintendent or designee 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. They 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 technology to access the Internet in accordance with the District's Network and Internet Acceptable Use Policy unless otherwise directed by a member of the staff. Staff supervising students using District technology shall help to monitor student online activities in accordance with the District's Internet Safety Policy and this regulation**.**
- The Superintendent, or designee, 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 harmful, inappropriate or unlawful activities.

IV. Training

The District shall provide training to staff and students on the requirements of the Internet Safety Policy and this regulation.

- The training of staff and students shall highlight the various activities prohibited or restricted by the Internet Safety Policy and the responsibility of staff to monitor student online activities to ensure compliance.
- The District shall also provide age-appropriate instruction to students regarding appropriate online behavior. Such instruction shall include, but not be limited to: positive interaction 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.
- Instruction will be provided even if the District prohibits students from accessing social networking sites or chat rooms on District computers
- Students shall be directed to consult with their classroom teacher if they are unsure whether their contemplated activities are consistent with District policy, regulation and/or student handbook.
- Staff and students will be advised not to disclose, use, and disseminate personal information about students when accessing the Internet or engaging in authorized forms of direct electronic communications as explained in further detail in policy 8635 Information and Data Privacy Security, Breach and Notification.

- District technology may not be used to engage in activities in violation of the District Code of Conduct.

The Commissioner of Education shall provide technical assistance to assist in the development of curricula or instruction for such course of study which shall be age-appropriate and developed according to the needs and abilities of students as successive grade levels in order to provide awareness, skills, information and support to aid in the safe usage of the Internet.

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, restriction of access, the revocation of technology access privileges, as well as school suspension in the case of students as set forth in the Code of Conduct and disciplinary charges and/or other penalty as set forth in an applicable collective bargaining agreement in the case of staff.
- In the event that the violation is more significant, it should be reported to the Superintendent or their designee.

Cross-ref: 4526, Network and Internet Acceptable Use Policy
8635 Information and Data Privacy 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

Education Law § 814
47 USC §254(h), (l)
20 USC §6*777*
47 CFR §§54.500 et seq.

Policy Adopted: May 9, 2002
Amended: 10/22/08; 8/7/12; 7/7/15, 1/17/18, 5/22/19, 6/16/21, 7/5/23, 6/12/24, 5/14/25, 6/17/26

Annual Review: 6/18/13; 6/18/14, 6/15/16, 6/14/17, 6/17/20, 6/16/21, 6/15/22, 7/5/23, 6/12/24, 5/14/25, 6/17/26

Effective: 7/1/26

Hewlett-Woodmere UFSD **Regulation 4526.1-R**

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 (a) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (b) such visual depiction 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 (c) such visual depiction 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 designee shall secure information about, and ensure the purchase or provision of, a technology protection measure that blocks access from all district computers to visual depictions on the Internet that are obscene, child pornography or harmful to minors.

- The Director of 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 Director of Technology or designee may disable or relax 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 Director of Technology shall monitor the online activities of adult staff members for whom the blocking and filtering technology measure 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

- The Director of 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. They 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.

- 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 coursework.
- 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 Director of 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 Director of Technology shall provide training 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.

- The 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 when accessing the Internet or the Worldwide Web are directly related to their course work.
- Staff and students will be advised not to disclose, use, and 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 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.

Adoption date: June 15, 2022
Amended: 6/12/24, 6/17/26

Effective: 7/1/26