INTERNET SAFETY POLICY

It is the policy of the Bethlehem Central School District (the "District") to comply with the Children's Internet Protection Act of 2001 and the Protecting Children in the 21st Century Act of 2008 (collectively, the "Internet Safety Laws").

The District recognizes that the Internet Safety Laws require the District to undertake reasonable efforts to:

- Block or filter access to certain material, including obscene pictures, child pornography, and other material harmful to minors;
- Monitor online activities of minors; and
- Educate minors concerning appropriate online behavior.

In addition, all use of District Technology to access the Internet must comply with the District's Technology Resources and Data Management Policy and Regulation (8630/8630-R) and Acceptable Use Policy and Regulation (4526/4526-R).

As set forth in the District's Acceptable Use Regulation, the District cannot guarantee that technological measures will prevent minors from accessing inappropriate content. The District will educate students about appropriate online behavior. Parents and guardians are expected to supervise and monitor students' use of the Internet when children are using District Technology outside of school.

The superintendent of the District is hereby directed to establish a Regulation setting forth appropriate procedures and procure appropriate technology to comply with the Internet Safety Laws and the District's Acceptable Use Policy. These procedures and technology shall include:

- Acquisition and deployment of Internet blocking and/or filtering software;
- Monitoring of online activities facilitated by District Technology;
- Restrictions on disclosure of students' personal information online;
- Restrictions on unauthorized online access by students, including hacking and other unlawful activities; and
- Education and training on safety and security of minors relating to the use of email, chat rooms, and other online communications.

Consistent with the Internet Safety Laws, the superintendent's Regulation also shall establish appropriate procedures to allow exceptions to this Internet Safety Policy for adults conducting bona fide research or other lawful activities.

Cross-Reference	1130.1 Social Media Guidelines 4526 Acceptable Use 8630 Technology Resources and Data Management 8635 Information Security Breach & Notification
Rescinds:	4526.1 Internet Safety
Adoption Date:	August 9, 2017

INTERNET SAFETY REGULATION

This Internet Safety Regulation establishes the general guidelines for use of the Internet pursuant to the Internet Safety Policy No. 4526.1 established by the Bethlehem Central School District (the District).

I. Definitions

A. *Capitalized Terms*. Unless otherwise stated herein, all capitalized terms shall have the same definitions as those set forth in the District's Internet Safety Policy (4526.1) and Acceptable Use Policy (4526).

B. *Child Pornography*. Any visual depiction, including any photograph, film, video, picture, 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. Child Pornography also includes any such visual depiction that:
   1. is or appears to be, of a minor engaging in sexually explicit conduct;
   2. has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or
   3. is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

C. *Harmful to Minors*. Any picture, image, graphic image file, or other visual depiction that:
   1. taken as a whole and, with respect to minors, appeals to the prurient interest in nudity, sex, or excretion;
   2. 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 sex acts, or a lewd exhibition of the genitals; and
   3. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

D. *Obscene*. Any picture, image, graphic image file, or other visual depiction that:
   1. the average person, applying contemporary community standards, would find the image, taken as a whole, appeals to the prurient interest;
   2. describes, in a patently offensive way, sexual conduct; and
   3. taken as a whole, lacks serious literary, artistic, political, or scientific value.

II. Mandatory Blocking and Filtering Measures

A. As set forth in Policy #8630, the superintendent, or his or her designee, shall secure information about, and ensure the purchase or provision of, a technology protection measure that blocks access to visual depictions on the Internet that:
   1. as to adults, are obscene or child pornography; and
   2. as to children, are obscene, child pornography, or harmful to minors.

B. The District's director of Technology (DOT) shall be responsible for the installation and proper use of any blocking or filtering measure obtained by the District.

C. The DOT and/or his or her designee may disable or relax the District's Internet blocking and filtering technology only for adult staff members conducting research related to the discharge of their official responsibilities. In such cases, the DOT and/or his designee shall monitor the activities of adult Users for whom the blocking and filtering technology measure has been disabled to ensure that such Users are not accessing prohibited materials.

III. Monitoring of Online Activities

A. The DOT shall be responsible for monitoring to ensure that online activities of Users are consistent with the District's Internet Safety Policy, this Regulation, and the District's Acceptable Use Policy and Regulation.

B. The DOT may inspect, copy, review, and store at any time, and without prior notice, any and all usage of District Technology for accessing the Internet, as well as any and all information transmitted or received during such use.

C. During the school day and/or at school events, staff are authorized to monitor student use of District Technology.

D. Parents and/or guardians of students bear the responsibility for setting and conveying standards that their children should follow when accessing the Internet, both inside and outside of school. In addition, parents and/or guardians may opt out of allowing their children to access the Internet using District Technology.

E. Parents/guardians must supervise and monitor student use of District Technology outside of school to ensure such use complies with the Internet Safety Policy, this Regulation, and the District's Acceptable Use Policy and this Regulation.

IV. Training

A. The DOT 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.

B. The training of Users shall highlight the various activities prohibited by the Internet Safety Policy and the responsibility of staff to monitor student online activities.

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

D. Students shall be directed to consult with their classroom teacher if they are unsure whether their contemplated activities when accessing the Internet are appropriate.

E. Users will be advised that unauthorized access (hacking) and other unlawful activities are prohibited.

F. Users will be advised not to disclose, use, or disseminate personal information about students when accessing the Internet or engaging in authorized forms of direct electronic communication.

G. Users will be informed of the range of possible consequences attendant to a violation of the Internet Safety Policy and this Regulation.

V. Violations

A. Violations of the Internet Safety Policy and this Regulation shall be reported to the building principal who shall take appropriate action in accordance with authorized disciplinary procedures set forth in the District's Acceptable Use Policy or other applicable policies.

B. Penalties for students may include, but are not limited to, the restriction or revocation of computer access privileges, suspension, and other discipline consistent with the Code of Conduct.

C. Penalties for staff and other authorized users may include, but are not limited to, revocation of computer access privileges and other discipline allowed pursuant to contract and/or law up to and including termination.

D. In addition, the District may pursue legal options for damage to District Technology or Data, or for other damages suffered by the District.

E. Violations that appear to be criminal in nature will be reported to the appropriate law enforcement authorities.

Adoption Date: August 9, 2017