INTERNET SAFETY
ACCEPTABLE USE POLICY

The Board of Education is committed to complying with the Children's Internet Protection Act and to undertaking efforts that serve to make safe for children the use of district computers 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 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 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 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 obscene, child pornography or harmful to minors.

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 and World Wide Web. The Superintendent or his or her designee shall establish and implement procedures that enforce these restrictions.

The Director of Technology 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 on their requirements.

All users of the district's computer network, 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 and accompanying regulation, in addition to generally accepted rules of network etiquette (see list of prohibited activities and uses, below) and the district's Acceptable Use Policy. Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges.

Users of the district's computer network have no reasonable expectation of privacy on the internet. The District reserves the right to access and view any material stored on District equipment or any material used in conjunction with the District's network and computers.

PROHIBITED ACTIVITIES AND USES

The following is a list of prohibited activity concerning use of the District computer network. Violation of any of the following prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the network.

1. Using the network for commercial activity, including advertising.

2. Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the District computer network.

3. Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material.

4. Using the network to receive, transmit or make available to others messages that are threatening, obscene, racist, sexist, abusive or harassing to others.

5. Using another user's account or password.

6. Attempting to read, delete, copy or modify the documents.

7. Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.

8. Using the network to send anonymous messages or files.

9. Using the network to receive, transmit or make available to others a message that is inconsistent with the District's Code of Conduct.

10. Revealing the personal address, telephone number or other personal information of oneself or another person.

11. Using the network for sending and/or receiving personal messages.

12. Intentionally disrupting network traffic or crashing the network and connected systems.

13. Installing personal software or using personal disks on the District's computers and/or network without the permission of the appropriate District official or employee.

14. Using District computing resources for commercial or financial gain or fraud.

15. Stealing data, equipment or intellectual property.

16. Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, or vandalize the data of another user.

17. Wastefully using finite District resources.

18. Changing or exceeding resource quotas as set by the District without the permission of the appropriate District official or employee.

19. Using the network while access privileges are suspended or revoked.

20. Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

21. Downloading materials from the Internet without permission.

22. Disrupting the use of the Internet by others.

23. Failing to abide by any licensing agreements.

24. Using abusive or offensive language, including the use of vulgarities, swearing, and name-calling.

25. Purchasing items via the Internet or subscribing to commercial services.

26. Bypassing or hindering security measures.

27. Using the Internet in any illegal manner.

28. Accessing, transmitting, or re-transmitting material which permits or advocates violence of any kind or advocates destruction of property.

29. Using encryption software.

30. Accessing the Internet using a non-District account.

31. Using the Internet during prohibited times.

32. Using the system to hinder the ability of others to work, to harass, intimidate, or annoy any other person.

Ref: Public Law No. 106-554
47 USC §254
20 USC §6801

Adoption date: September 9, 2015

INTERNET SAFETY ACCEPTABLE USE AND CONSENT FORM

The Eastport-South Manor Central School District is requesting consent for your child to use telecommunications in the School District, including the use of the Internet. Consent is required before your child will be permitted to use telecommunications in the School District. Please read this document in its entirety before signing the consent form.

The development and maintenance of excellent educational and instructional programs are of primary importance to the Eastport-South Manor Central School District. It is the belief of the District that technology and Internet access provide unique and meaningful opportunities to support teaching and learning.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. While we believe that the benefits for children who have access to the Internet far outweigh any potential risk, it should be understood that some sites might contain information that is inappropriate, pornographic, defamatory, inaccurate, or potentially offensive to some users. While the District will attempt to prevent student access to these types of materials, the District cannot assure that a user of the Internet will not be able to discover this material.

The Eastport-South Manor Central School District believes strongly in promoting the ethical use of technology. We have therefore set forth the following guidelines for all to follow:

1. I will limit my use of telecommunications in school to the educational objectives established by my teacher(s);

2. I will not retrieve or send illegal, obscene, offensive, pornographic or other sexually explicit material that is not within the school's established curriculum;

3. I will not use abusive language or vulgarities of any type, including swearing and name-calling;

4. I will not divulge my own or anyone's address, phone number or any other personal information to any person for any purpose, and will report any requests of this kind to my classroom teacher, librarian or principal;

5. I will not plagiarize information received in any form and will properly cite all materials;

6. I will not use another person's account or password to access the Internet;

7. I will not share my password or account information with anyone;

8. I will not download any material from the Internet without the consent of my teacher(s) or school personnel;

9. I will not attempt to bypass security built into the system;
10. I will not vandalize network materials, services, traffic, equipment, and software, or attempt to download a virus from the Internet;

11. I will not use Internet access for illegal purposes of any kind;

12. I will not use Internet access to transmit threatening, obscene, sexist, racist, abusive, or harassing materials;

13. I will not use school computers to chat online, send e-mail or text messages, personal messages and/or instant messages unless I have received permission from a teacher and the use is part of a teacher's supervised activity;

14. I will abide by the licensing agreements for any school subscriptions and online databases, which require a user name and password;

15. I will not download, upload, or duplicate any copyrighted materials or material protected by applicable copyright law, or other intellectual property rights laws;

16. I will not use the system for commercial solicitation;

17. I will not purchase items via the Internet or subscribe to commercial services, and shall be responsible for any and all charges due for such purchases;

18. I will report any known security risks to a teacher;

19. I will report any threatening or obscene materials, expressions of racism or hate, or other materials which are intended to embarrass, harass or disrupt the education environment of the school to a teacher;

20. I will not disrupt the use of the network by other users;

21. I will not send anonymous messages to anyone through the Internet;

22. I will not access, transmit, or retransmit material which permits or advocates violence of any kind or advocates destruction of property;

23. I will not use encryption software from any access point within the School District;

24. I will not access the Internet using a non School District Internet account;

25. I will use the Internet only during permitted times during and/or before and/or after the school day;

26. I will not use the computer network system to hinder the ability of others to work, to harass, intimidate, or annoy any other person;

27. I will not install personal software or use personal disks on District computers without permission;

28. I will not use the system to gain or seek to gain unauthorized access to any files, resources, or computer or telephone system, or vandalize the data of another;

29. I will not wastefully use District resources;

30. I will not use the computer network or Internet while my privilege to do so is suspended or revoked;

31. I will not use the network to receive, transmit or make available to others a message that is inconsistent with the District's Code of Conduct;

32. I will not use the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

The use of the Internet is a privilege, not a right. Any inappropriate use will result in a cancellation of the privilege. Users have no reasonable expectation of privacy on the Internet. The District reserves the right to access and view any material stored on District equipment, or any material used in conjunction with the District's computer network.

The School District reserves the right to monitor all Internet activity by students. Any violation of the foregoing guidelines will be treated as a violation of the Student Discipline Code, and shall be handled according to such discipline code. Any violation may also result in the loss of Internet privileges. The School District shall notify the appropriate legal authorities if there is suspicion of illegal activities. The system administrator shall determine whether student conduct constitutes a violation of the guidelines and his/her decision shall be final.

Users of the District's computer network should not expect, nor does the District guarantee, privacy for any use of the District's computer network. The District reserves the right to access and view any material stored on District equipment or any material used in conjunction with the District's computer network. The District may monitor all use of the District's computer network and the Internet.

The Eastport-South Manor Central School District makes no warranties of any kind, whether express or implied, for the Internet service it is providing. The District shall not be responsible for any damages suffered. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or a user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

The Eastport South Manor Central School District recognizes that technology represents an integral component to 21st Century Digital Age Learning for our students. To that end, students and staff are permitted to bring their own personal computing devices to school for educational purposes, in accordance with the district's Acceptable Use Policy. While students and staff are permitted to bring their own personal computing devices to school, they are not a necessary part of the educational program. No student's learning experience or academic performance will be affected because he or she does not have a personal computing device.

Students and staff choosing to use their own personal computing devices in school are responsible for their own equipment. The district will not service or repair any device that is not owned by the district and is not responsible for any loss, theft, damage, and/or malware that may occur to student-owned devices. Acceptable devices will include such items as tablets, laptops, iPads, e-Readers, and Smartphones. Students will be responsible for charging their device before the school day and will not be provided access to electric/power stations. Students will understand that the classroom teacher has the authority to determine when the use of personal computing devices is or is not appropriate. All student and staff-owned devices will require advanced registration prior to accessing the district's wireless network and Internet. Under no circumstances will students be permitted to use their personal computing devices using any other broadband or wireless network.

STUDENT STATEMENT:

I, _____, have read the Eastport-South Manor Central School District's Internet Use Policy, the District Internet Safety and Use Guidelines and the Internet

Use and Consent Form and understand that any failure on my part to follow these guidelines will result in appropriate disciplinary action and possible loss of access privileges to the Internet.

Signed: _____ Date: _____

PARENT/GUARDIAN STATEMENT:

I, _____, have read the Eastport-South Manor Central School District's Internet Use Policy, the District Internet Safety and Use Guidelines and the Internet Use and Consent Form, in consideration of the privilege of my child's use of the District's technology systems and in consideration of my child's having access to the Internet, I hereby release the District, its officers, employees, operators, and any institutions with which they are affiliated, from any and all claims and damages of any nature arising from my, or my child's use, or inability to use the system. I recognize it is impossible for the District to restrict access to all inappropriate educational materials and I will not hold it responsible for materials acquired on the Internet. I accept full responsibility for supervision if and when my child's use is not in a school setting. I also accept full responsibility and liability for the results of my child's actions with regard to the use of the Internet. I release the District from any liability relating to consequences resulting from his/her use of the Internet. I give permission to issue an account for my child, who I understand has read and/or reviewed with me the foregoing and understands his/her responsibilities regarding acceptable internet use.

Signed: _____ Date: _____

STAFF STATEMENT:

I, _____, have read the Eastport-South Manor Central School District's Internet Use Policy, the District Internet Safety and Use Guidelines and the Internet

Use and Consent Form and understand that any failure on my part to follow these guidelines will result in appropriate disciplinary action and possible loss of access privileges to the Internet.

Signed: _____ Date: _____

Adopted: September 9, 2015

INTERNET SAFETY
ACCEPTABLE USE POLICY 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 and World Wide Web.

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.

II. Blocking and Filtering Measures

- 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 from all district computers to visual depictions on the Internet and World Wide Web 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 his or her 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 computer network coordinator 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. 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 World Wide Web 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, students may use the district's computer network 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 district computers shall help to monitor student online activities to ensure students access the Internet and World Wide Web, 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 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 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.

- Students shall be directed to consult with their classroom teacher if they are unsure whether their contemplated activities when accessing the Internet or Worldwide Web 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.

- 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: September 9, 2015