Policy
Board of School Trustees
Program
East Noble School Corporation
Revised June 2020

EAST NOBLE SCHOOL CORPORATION
STUDENT RESPONSIBLE USE POLICY

All use of the Internet shall be consistent with East Noble School Corporation's goal of inspiring, engaging, and empowering all learners by facilitating resource sharing, innovation, and communication. Guidance and digital citizenship instruction will be provided and required for each individual granted Internet access through the school. The policy does not attempt to state all required and/or unacceptable behaviors by users. However, some specific examples are provided. The failure of any user to follow the terms of the Responsible Use Policy for Internet Access will result in the loss of privileges, disciplinary action and/or appropriate legal action. An agreement to this form is legally binding and indicates the party who signed off has read the terms and conditions carefully and understands their significance.

Internet - Terms and Conditions

1) **Acceptable Use** - The use of your account must be in support of education and research and consistent with the educational objectives of East Noble School Corporation.

2) **Privileges** - The use of the East Noble telecommunications services is a privilege, not a right. Inappropriate use will result in the cancellation of those privileges. The chief technology officer and the superintendent will deem what is inappropriate use and their decision is final. The administration, faculty, and staff of East Noble School Corporation may request the CTO and/or the system administrators to deny, revoke, or suspend specific user accounts. Students will be issued a school email address to improve student communication and collaboration on school projects. Email shall be used only for educational purposes that directly relates to a school project or assignment.

3) **Unacceptable Use –** You are responsible for your actions and activities involving the network. Some examples of unacceptable use are:

- Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or state regulation.
- Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused.
- Downloading copyrighted material
- Using the network for private or commercial advertising or gain.
- Gaining unauthorized access to resources or entities, including hacking.
- Invading the privacy of individuals.
- Posting material authored or created by another without his/her consent.
- Posting anonymous messages.
- Accessing, submitting, posting/publishing or displaying defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing or illegal material, or any other material deemed educationally inappropriate.
- Using the network while access privileges are suspended or revoked.
- Posting chain letters or engaging in spamming.

3) **Exclusive Use of Access** - Network users are solely responsible for the use of their logins, passwords, and access privileges. Any problems that arise from the use of a registered user's login are the user's responsibility. The use of a registered login by someone other than the user is forbidden and is grounds for denial or limitation of network access privileges. Primary network resources can only be accessed with school owned computers, laptops and similar devices. The use of cell phones is defined by each building, and users should understand and follow those guidelines provided elsewhere. An appropriately-trained administrator may examine a student's personal telecommunication device and search its contents, in accordance with disciplinary guidelines. Students are encouraged to use cloud storage to store files between classrooms, home and school.

4) **Technology Protection Measures** – Access to inappropriate materials as defined by school policy and the Children's Internet Protection act is prohibited. Steps shall be taken to promote the safety and security of users of the East Noble School Corporation computer network with using electronic mail, chat rooms, and other forms of direct communication. East Noble installs FortiClient computer filtering software on all devices to prevent the on-screen depiction of obscenity, child pornography, or other material harmful to minors. Any attempts to circumvent this filter will result in loss of privileges or disciplinary action.

5) **Network Etiquette** – You are expected to abide by the accepted rules of network and safety etiquette. These include but are not limited to the following:

- Be polite.
- Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
- Do not disclose, use, or disseminate the personal information of yourself or others. Student data must remain confidential in accordance with the Family Education Rights and Privacy Act (FERPA) and the Children's Internet Protection Act (CIPA).
- Do not use the network to disrupt the use of the network by other users.
- All communications and information accessible via the network should be assumed to be property of East Noble School Corporation.

6) **Personal Safety –** For your own benefit, observe the following precautions:

- Do not post personal contact information about yourself or other people. This information includes, but is not limited to, your address, telephone number, work address, etc.
- Do not agree to meet with someone you have met online.
- Disclose to your teacher, librarian, or classroom supervisor any message you receive that is inappropriate or makes you feel uncomfortable.

7) **Search and Seizure/Due Process** - Your laptop and network accounts are not private. Routine maintenance and monitoring of the email or file servers may lead to discovery that you have violated this agreement, or the law. The chief technology officer and/or systems administrators will conduct searches if there is reasonable suspicion that you have violated this agreement or the law, or if requested by local, state or federal law enforcement officials. East Noble will cooperate fully with local, state, or federal officials in any investigation related to illegal activities conducted on network resources owned by East Noble School Corporation.

8) **Security** - Security on any computer system is of the highest priority, especially when the system involves many users. If you identify a security problem on technology resources, you must notify the chief technology officer. Users should not demonstrate the problem to other users. Users should not use another individual's logins. Attempts to log on to the network with a stolen identity or as a system administrator will result in cancellation of user privileges and possible expulsion. If a user is identified as a security risk or has a history of problems with other computer systems, East Noble Schools may deny access to technology resources.

9) **Vandalism/Harassment** – Vandalism and/or harassment will result in cancellation of privileges and disciplinary action will be taken. Vandalism is defined as any malicious and/or intentional attempt to harm, steal or destroy data of another user, school networks, or technology hardware. This includes but is not limited to the uploading or creation of computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent network security. Harassment is defined as the persistent annoyance of another user or the interference in another's work. This includes, but is not limited to, the sending of unwanted e-mail.

10) **Digital Citizenship and Cyberbullying** – School staff will educate students about appropriate and safe online behavior, including interacting with individuals on social networking sites and in chat rooms and cyberbullying awareness and response. Cyberbullying will not be tolerated. Exclusion, harassment, outing, cyberstalking, frapping, creating fake profiles, dissing, and trickery are all forms of cyberbullying and are forbidden. Users should not send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors or any online activities intended to harm (physically or emotionally) another person will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Students should remember that activities are monitored and retained.

11) East Noble School Corporation reserves the right to amend this policy as needed.

12) The Responsible Use Policy is signed off on each year while at East Noble School Corporation.