Internet Safety Policy

These guidelines are intended to ensure the safe and secure use of the internet by students, encompassing various devices and online activities.

Internet Privacy and Security Board

Sam Johson	Director of Operations
Charles Thacker	Secondary Assistant Principal
Cathy Carver	Secondary Assistant Principal
Dottie Trapnell	Elementary Assistant Principal
Jacob Green	IT Specialist

1. Filtering and Content Restrictions: The school employs an in-house web filtering system called "Red-Handed" to ensure a safe online environment for students. Red-Handed filters websites based on various criteria, including but not limited to, social media, explicit content, drugs, violence, and adult material. Access to websites considered inappropriate or harmful is restricted. The aim is to create a productive and secure digital space for learning. The school's internet filtering practices are fully compliant with the Children's Internet Protection Act (CIPA).

2. Email Communication: Student email accounts are limited to communication within the school's network. External communication is restricted to ensure a focused and secure educational environment. This measure is taken to prevent unsolicited emails and potential security risks.

3. Software Installation and Execution: Student devices are configured to prevent the installation of unauthorized software and the execution of arbitrary executable programs. This ensures the integrity of the devices and minimizes the risk of malware, viruses, or disruptions to the educational process.

4. Student Data Privacy: Any student data shared with software providers is subject to a student data privacy agreement. This agreement outlines how the data will be used, protected, and maintained by the software providers in compliance with personally identifiable information (PII) regulations, the Family Educational Rights and Privacy Act (FERPA), and the Children's Internet Protection Act (CIPA). To review the details of any of the student data privacy agreements, please visit https://rgsa.com/internet-policy.

5. PII Inquiry and Resolution Protocol: In line with our dedication to data privacy, we have established a protocol for addressing concerns related to personally identifiable information (PII). As per our practices, any inquiries or issues pertaining to PII are promptly directed to the Internet Privacy and Security Board, the designated authority for handling such matters. This approach ensures that student data remains confidential and that any questions regarding its usage are addressed in accordance with established guidelines and regulations.

6. Compliance with the Student Online Personal Information Protection Act: Our requirement for online services is that they adhere to the following guidelines:

- **Minimal PII Collection:** Online services should only gather the minimal amount of Personally Identifiable Information (PII) necessary to fulfill K-12 objectives.

- **Stringent Security Measures:** Online services must implement robust security protocols to guard against unauthorized access and the inadvertent disclosure of information.
- **Prohibited Usage and Sharing:** PII collected cannot be used for advertising or commercial purposes, and it cannot be shared, rented, or sold to any third parties.
- **Timely Data Deletion:** Online services are required to delete PII within 90 days after a student concludes enrollment, unless explicit parental consent for data retention is obtained.

7. Parent Notifications and Policy Updates: For privacy (PII) and policy changes, detailed information will be provided through these channels.

- **Phone Call:** Swift updates, prioritizing urgent matters.
- **Email:** Event details and policy changes.
- **Paper Notices:** Important updates sent home with students.

8. Staff Oversight and Approval: All staff members are required to review and approve websites and software before allowing student access. In cases where a specific online resource is blocked, staff must request its unblocking from the Internet Privacy and Security Board. This practice ensures that all online resources are in line with the school's educational goals and adhere to established content guidelines. It also empowers staff to make informed decisions about the suitability and relevance of digital resources, maintaining a secure and productive online learning environment for students.

9. Prohibited Platforms: TikTok and any successor platforms are strictly prohibited and blocked from being used on any devices provided by the school. This measure is in place to maintain a distraction-free and safe online learning environment.

10. Personal Devices on School Network: Personal devices are not allowed to connect to the school's network. This policy helps maintain network security, prevent potential disruptions, and ensures a controlled digital environment for learning.

11. No School Promotion on TikTok or Successor Platforms: The school will never use TikTok or any successor platform to promote the school, school-sponsored clubs, extracurricular organizations, or athletic teams. This ensures that the school maintains a professional and consistent image across all digital platforms.

By adhering to these guidelines, we aim to create a secure, focused, and productive online environment for all students. If you have any questions or concerns about this policy or its compliance with CIPA, please feel free to contact the school administration.

This policy is effective as of 9/1/2023 and is subject to periodic review and updates as needed.