STUDENT INTERNET SAFETY POLICY

COMPLIANCE WITH THE CHILDREN'S INTERNET PROTECTION ACT

As technology continues to advance, the safety of school children online is a matter of public concern and an issue of the highest importance to School Districts, the Department of Education, and the school districts in your State. The purpose of this policy is to protect District students from inappropriate material online while still fostering and promoting the use of technology in the learning process. This policy is designed to be enforced in conjunction with the District's technology acceptable use policy and is specifically adopted to comply with and exceed the requirements of the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC § 254(h)] and the implementing regulations of the Federal Communications Commission. The Children's Internet Protection Act ("CIPA") was enacted by Congress to address concerns about access to obscene or harmful content over the Internet by children.

In compliance with CIPA, and to the maximum extent permitted by law, students and employees in this District are not permitted to obtain, download, view, or otherwise gain access to inappropriate matter on District technology or through the District's Internet. Inappropriate matter includes materials that may be deemed unsuitable for minors, unlawful, abusive, obscene, pornographic, or otherwise objectionable under current District policy or legal definitions.

Technology Protection Measure

In compliance with CIPA, the District will ensure that a District-wide technology protection measure (content filter) is established and effectively working to protect against Internet access on District technology by both adults and minors to visual depictions that are obscene, pornographic, or harmful to minors.[1]

It is of utmost importance to this District that content filters are effective while students have access to the Internet on District-owned devices and that this policy is strictly followed. Therefore, the District's content filter and its effectiveness should be reviewed once a month by District technology personnel and/or the appropriate administrator and will be subject to random checks for effectiveness by an appointed member of the Board of Education.

The use of any District technology to access sites which allow the user to conceal their objective of accessing inappropriate material is not permitted. Employees or students using technology to circumvent the content filter in order to access unauthorized or prohibited websites will be subject to discipline. The content filter may only be disabled by an appropriate administrator during use by an adult to enable access for bona fide research or other lawful purpose.

Additionally, as content filters are not enough to protect students online and offline, the District will purchase and maintain software to measure the effectiveness of the content filter and

[1] As defined pursuant to 45 C.F.R. § 54.520(a).

monitor student use of computers to assist in warning the District of inappropriate online activities of students.

Internet Safety Training

In compliance with CIPA, each year, all District students will receive Internet safety training which will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response. Such training will encompass safety measures for usage of the Internet, cell phones, text messages, chat rooms, email and instant messaging programs and stress the importance of maintaining the confidentiality of personal information online and the prevention of inappropriate network usage. Specifically, as required by CIPA, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

The training should be age appropriate and also focus on the proper use of technology at home, whether on school or personally owned devices. Options for completing this training include development of individual curriculum by District teachers or technology personnel or through purchase of training materials designed for compliance with CIPA.

The District will collect a sign-in sheet reflecting student attendance at annual CIPA trainings and will maintain these sign-in sheets for three years.

Students issued District-owned devices will sign a certification that they will exercise good faith to prevent inappropriate Internet usage, they will not circumvent technology prevention measures, they understand that their District-owned device will be monitored, they understand the safety risks associated with online activities, and they can be disciplined for failing to comply with District safety standards.

Annually, the District will provide at least one training session with, at a minimum, all administrative and teaching staff about student online safety, the requirements of CIPA, the District's content filters, and the importance of monitoring student Internet usage. The District will maintain a sign-in sheet from this training for three years.

Supervision and Monitoring

The District will be proactive in safeguarding students utilizing the District's Internet and technology and will comply with the requirement of CIPA to monitor the online activity of minors. District monitoring will include, but not be limited to, G-Suite and Google Chrome Browsers provided by the District. It shall be the responsibility of all District employees to supervise and monitor usage of the District's online computer network and access to the Internet in accordance with this policy and CIPA.

As content filters are not enough to keep students safe online, the District will maintain student safety and computer monitoring software that provides the tools to effectively monitor student activity on school owned computers as well as activities utilizing the District's Google tied school e-mail account (G-Suite). Such software detects inappropriate and unsafe activity beyond the capabilities of the District's filter system by containing libraries of key words and phrases that, when detected, cause a screenshot to be taken for further review by school administrators. Such technology allows schools greater insight into how computers are being used and how effective currently policies and technologies are at meeting state and federal requirements.

Any school district employee or student accessing their school district-provided Gmail and/or Google account will be monitored when using a Chrome Browser regardless of whether they are using a school district provided device or the users personal device. For any personal activity occurring off school premises it is strongly advised that users log out of the school district provided account. Users utilizing the school district provided Google account will be monitored and held responsible for any activity that is in conflict with the school district Policy for internet access. Use of the District-provided Gmail and/or Google account when using a Chrome Browser irrespective of ownership of the device will be deemed student/i.e. user consent to District monitoring.

The software system will detect at a device level and report on devices at a school level when words or phrases indicate potential bullying, threats, sexual, lewd, drug related and other unsafe issues. Monitoring reports will include tamper resistant evidence of inappropriate behavior, including device time, username, screenshot of the behavior, and whether such behavior was typed or viewed.

Each school building will appoint an administrator to review data collected by the monitoring software at least one hour per week with a focus on the most severe data collected and will intervene when inappropriate online and offline behavior is observed. It is encouraged that less severe data be maintained for later review.

The District will also monitor District-issued devices utilized by District students off school grounds via monitoring software and random checks of District-issued devices

The overriding goal of the District's monitoring and compliance system is to provide District students with a quality education free from depictions of material deemed to be obscene, pornographic, bullying as well as other material harmful to minors.

Audit by the State

The District understands the high importance of this issue and understands that maintaining documentation regarding compliance with this policy is critical as the District will be subject to an audit by the Office of the State Auditor (or equivalent) or the FCC. The District may be subject to penalties for noncompliance with this policy.

Community Involvement

The District will provide information about this Internet safety policy and its content filter and monitoring software to the community and annually hold one community program/forum about this policy to inform parents and patrons about student safety online.

Privileges & Notification of Monitoring

The use of District technology and electronic resources is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges.

Access to electronic mail (E-mail) and the District's Internet is a privilege and designed to assist students and employees in the acquisition of knowledge and in efficiently communicating with others. The District E-mail system is designed solely for educational and work related purposes. ***E-mail, Internet history, and files on District computers or accessed through District technology will be monitored and are subject to review by District and school personnel.***

Access to the Internet

In compliance with the Children's Internet Protection Act, the District uses a technology protection measure designed to filter and block the use of any District computer with Internet access to retrieve or transmit any visual depictions that are obscene, pornographic, or "harmful to minors" as defined by CIPA and material which is otherwise inappropriate for District students.

Due to the dynamic nature of the Internet, sometimes Internet websites and web material that do not fall into these categories are blocked by the filter. In the event that a District student or employee feels that a website or web content has been improperly blocked by the District's filter and this website or web content is appropriate for access by District students, the process described below should be followed:

1. Follow the process prompted by the District's filtering software (or to remain anonymous, log in under log in name: 123anonymous) and submit an electronic request for access to a website, or:

2. Submit a request, whether anonymous or otherwise, to the District's Superintendent/the Superintendent's designee.

3. Requests for access shall be granted or denied within three (3) days. If a request was submitted anonymously, persons should either attempt to access the website requested after three days or log back in at 123anonymous to see the status of the request.

4. Appeal of the decision to grant or deny access to a website may be made in writing to the Board of Education. Persons who wish to remain anonymous may mail an anonymous request for review to the Board of Education at the School District's Central Office,

stating the website that they would like to access and providing any additional detail the person wishes to disclose.

5. In case of an appeal, the Board of Education will review the contested material and make a determination.

6. Material subject to the complaint will not be unblocked pending this review process.

In the event that a District student or employee feels that a website or web content that is available to District students through District Internet access is obscene, pornographic, or "harmful to minors" as defined by CIPA or material which is otherwise inappropriate for District students, the Superintendent should be notified.

Adult users of a District computer with Internet access may request that the technology protection measures be temporarily disabled by the chief building administrator of the building in which the computer is located for lawful purposes not otherwise inconsistent with this policy.