Executive Summary
Prepared for Board of Trustees Meeting
June 8, 2021

Children's Internet Protection Act Compliance Status Update

***Board Goals*:**

- Teaching & Learning – Foster and support an advanced digital learning environment
- Culture & Climate – Promote mental health, physical wellness and social-emotional well-being
- Growth & Management – Demonstrate effective and efficient management of district resources
- Growth & Management – Provide leadership and/or oversight to ensure District meets all fiscal, legal and regulatory requirements

Purpose of Report

This report serves to update the Board of Trustees about the District's Children's Internet Protection Act (CIPA) compliance efforts.

Objectives

1. To publicly discuss the District's Internet Safety Policy
2. To document said discussion for USAC auditing to comply with E-Rate funding requirements
3. To inform new trustees of the District's Internet safety efforts, specifically regarding CIPA.

Operational Impact

CIPA Overview

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2011.

CIPA Requirements

CIPA requires the following:

- An Internet Safety Policy (ISP) describing school/library protection of minors from harmful/offensive material including:
    1. Access oversight and monitoring
    2. Technology Protection Measure (filtering)
    3. Education of minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response (since 2012 for schools only.)
- Public Notice of Hearing or Meeting-usually Board minutes of ISP reading/review and adoption.

Executive Summary
Prepared for Board of Trustees Meeting
June 8, 2021

Children's Internet Protection Act Compliance Status Update

DISD CIPA Policy

Denton ISD's CQ (Local) policy on Technology Resources contains an "Internet Safety" section which requires that the Superintendent develop implement an internet safety plan to:

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; and
5. Educate students about cyberbullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.

Filtering

Each District computer with internet access and the District's network systems shall have filtering devices or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent.

The Superintendent shall enforce the use of such filtering devices. Upon approval from the Superintendent, an administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose.

Results

In compliance with this policy, the District maintains

1. a URL filter to control students' access to inappropriate materials; this also meets the requirements of the "Filtering" subsection of the "Internet Safety" section of CQ (Local)
2. multiple email security platforms that provide a layered defense against malicious attachments, SPAM, spoofing, and phishing attempts to ensure student safety and security while using electronic communications.
3. access control policies to limit student access to critical infrastructure, web filters that block hacking as a category which limits access to tools and information related to hacking
4. Data Loss Prevention (DLP) policies for all email services with additional controls in place to stop the transfer of Personally Identifiable Information (PII) without encryption. (All security controls in place at the District are designed to protect student data while it is in use, at rest, and in motion. Staff is regularly trained on FERPA regulations and management of student data and PII.)
5. Common Sense Media curriculum to teach about online safety, privacy and security, digital footprint and identity, relationships and communication, cyberbullying, digital drama, and hate speech, news and media literacy, and media balance & well being.