



**CITY OF SANTA BARBARA**  
**LIBRARY BOARD REPORT**

**AGENDA DATE:** March 11, 2021  
**TO:** Library Board  
**FROM:** Administration Division, Library Department  
**SUBJECT:** CIPA Compliance

**RECOMMENDATION:**

That the Library Board receive SBPL's presentation on CIPA compliance including Cisco Umbrella and approve the proposed Internet Use and Safety Policy, attached.

**PREPARED BY:** Alain Dussert, Senior Librarian  
**SUBMITTED BY:** Kristina Hernandez, Library Services Manager  
**APPROVED BY:** Jessica Cadiente, Library Director





# Children's Internet Protection Act (CIPA)

The case for ensuring SBPL remains CIPA compliant.

# What is CIPA?

- 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.
- Libraries subject to CIPA may not receive the E-rate discounts unless they certify they have an Internet safety policy that includes technology protection measures.
- They may also be required to certify CIPA compliance in some grant applications.



# What CIPA Requires

- Adoption of an Internet Safety Policy with technology protection measures.
- Protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors).
- Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.
- An authorized person may disable the blocking or filtering measure during use by an adult to enable access for bona fide research or other lawful purposes.



# What Does an Internet Safety Policy Address?

- Access by minors to inappropriate matter on the Internet.
- Safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications.
- Unauthorized access, including so-called “hacking,” and other unlawful activities by minors online.
- Unauthorized disclosure, use, and dissemination of personal information regarding minors.
- Measures restricting minors' access to materials harmful to them.
- It should apply to both minors and adults.



# Technology Protection Measures

- Generally known as a web content filter.
- Filtering is required for all of an E-rate recipient's Internet-enabled computers whether used by minors or adults.
- For E-rate funding purposes, filtering for adult Internet usage can be disabled for "bona fide research or other lawful purpose."
- The FCC has not established any standards with regard to the type or effectiveness of Internet filters required for CIPA compliance.
- The filter's blocked and unblocked sites will iteratively change over time.



# Advantages of the Cisco Web Content Filter

- Cloud-based and affordable.
- Can filter all Black Gold Internet traffic on wired computers and through Wi-Fi access points simultaneously at all branches.
- Relies on the robust Cisco database of blacklisted and whitelisted sites.
- Allows customizable “blocked page” screens with timed bypass code features.
- Once implemented, is easy for all technology staff to operate.





# Recommendations to the Library Board

- SBPL recommends that the Library Board approve the proposed Internet Use and Safety Policy.
- This will enable SBPL to immediately become CIPA compliant.

