BLOCKSI

# Achieving CIPA Compliance on Chromebooks and Chrome Clients with

# Blocksi Manager Education Everywhere

## What is CIPA?

**The Children's Internet Protection Act (CIPA)** was signed into law on December 21, 2000. Schools and libraries that plan on utilizing E-rate discounts on Internet access and/or internal connection services after July 1, 2002 must be in compliance with CIPA. CIPA requires schools and libraries to filter their Internet services and have implemented formal Acceptable Internet Use Policies. The FCC administers CIPA for E-Rate purposes and provides general guidelines to achieve CIPA compliance. CIPA Requirements General Requirements for CIPA compliance require implementation of a technology protection measure (AKA Internet Filter), such as Blocksi Manager Education Everywhere (BMEE) and or Blocksi DNS . Schools must enforce a policy to monitor online activities of minors. To ensure CIPA compliance at all times, Internet access should be restricted when filtering technology is disabled.

### Key Topics To Be Covered

1. What does CIPA requires from an Internet content filtering ?
2. Categories for CIPA compliance.
3. Blocksi ensures CIPA compliance.
4. Monitor online activities of minors.

blocksi.net

sales@blocksi.net
228 Hamilton Avenue (3rd floor), Palo Alto, California 94301
1 877 693 4822

BLOCKSI

# 1- Internet Filter CIPA  Requirements:

• Block access to visual depictions deemed “obscene”, ”child pornography”, or “harmful to minors”

• Safety and security of minors when using direct electronic communications

• Filtering is required for all Internet-enabled computers whether used by minors or adults.

• Filtering of adult Internet usage can be disabled for research or other lawful purposes

• Block unauthorized access, including ‘hacking’, and other unlawful activities by minors online



sales@blocksi.net
228 Hamilton Avenue (3rd floor), Palo Alto, California 94301
1 877 693 4822

BLOCKSI

# 2- Categories For CIPA Compliance

In order to ensure CIPA compliance, managing access to the following is recommended:

Categories are recommended to meet CIPA compliance and not specifically identified as required by CIPA .

*Safe search for Image and videos sites is recommended if access to image or video sites is desired to be opened for minors.

Google Safe search Images, is recommended to ensure CIPA compliance and is enabled by default in Blocksi Manager Education Everywhere or in Blocksi DNS.

Blocksi Manager Education Everywhere offers a comprehensive set of tools and controls to ensure CIPA compliance beyond standard URL Filtering to expand security for applications, sharing, image searching, and YouTube.com Categories Controls include URL, Applications, Keywords, Content Type Threat & Event Reporter Store Internet and user activity logs for extended periods. In addition, dynamic access to this data is required to identify and resolve obscure threats lurking in the logs

## Web Categories

- Adult Content
- Alcohol/Tobacco
- Dating/Personals
- Drugs
- File Sharing
- Gambling
- Games
- Proxies
- Pornography/Nudity
- Guns/Weapons
- Violence/Hate
- Virus/Malware Safe Search
- Peer to Peer
- New Groups
- File Sharing
- Google Encrypted Access
- Dynamic Proxy Blocking
- Hot Spot Shield
- Rogue Encrypted Connections
- SSL Domain Enforcement
- Google Safe Image Search



sales@blocksi.net
228 Hamilton Avenue (3rd floor), Palo Alto, California 94301
1 877 693 4822

BLOCKSI

## Keywords Filtering

Web pages are scanned and if are let through for any reason through the web based category filtering because belonging to an allowed category, keyword filtering is able to block these pages which are deemed inappropriate.

## Youtube Filtering

- Strict Mode
- Youtube filtering across 20 cateories including the adult ones so that only the video that are appropriate are let through
- Youtube Strict and Moderate mode so that even within the allowed categories and channels; video which are miscategorized are getting blocked.
- Youtube channel filtering
- Youtube filtering by keyword description



sales@blocksi.net
228 Hamilton Avenue (3rd floor), Palo Alto, California 94301
1 877 693 4822

BLOCKSI

## Hotspot Shield

Even if a smartphone cellular data hotspot is being used, Blocksi Manager Education Everywhere enforces the school content filtering policy wherever the chromebook is located.

## Rogue VPN and rogue SSL

Even if the student manages to establish rogue vpn and ssl tunnel connection to a third party provider, Blocksi Manager enforces directly in the chrome browser the school content filtering policy



sales@blocksi.net
228 Hamilton Avenue (3rd floor), Palo Alto, California 94301
1 877 693 4822

BLOCKSI

# 3-Blocksi Manager Education Everywhere (BMEE) Ensures CIPA Compliance

BMEE provides the technology needed to ensure your network is CIPA compliant. Blocksi provides granular filtering tools with industry leading monitoring tools that simplify compliance and automate reporting. Additionally, the per GSuite organization units custom Blocksi extension gives the administrators the ability to enforce CIPA compliance to certain groups yet provide more open access to others on the network (i.e. teachers vs. students).

## Working With Your Support Engineer

Blocksi provides U.S. based support which will work with you one on one to go over configuration and ensure CIPA compliant categories are enforced. Additionally, your support engineer will review other filtering tools that may not be a direct requirement for CIPA compliance but may add to the security of your network.

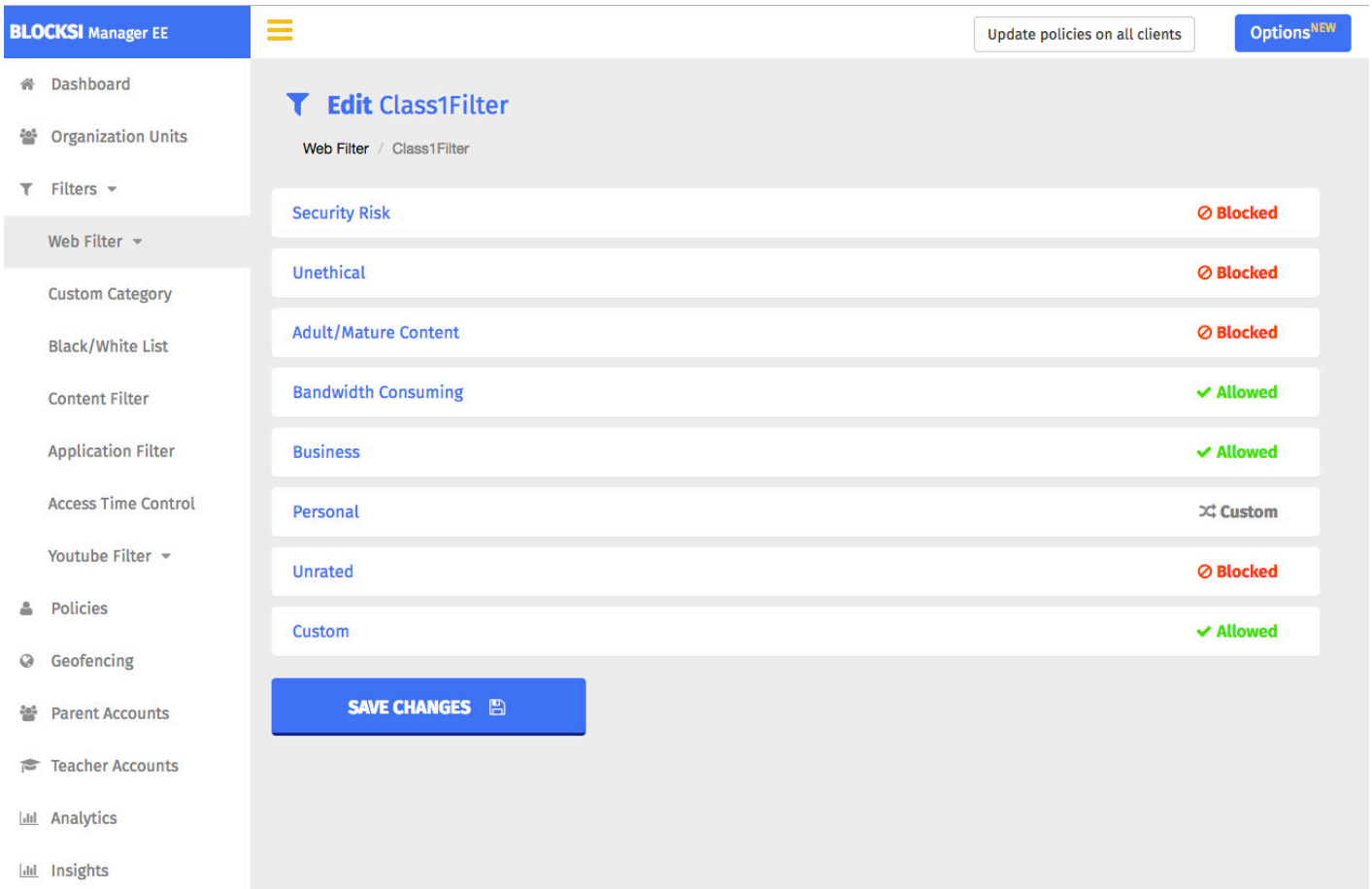
**Below are general outlines of selecting categories for CIPA compliance:**

1. Access the Blocksi Manager Education Everywhere Administrator Dashboard
2. Select Filter Apps
3. Select 'Web Filters' and create a Web Filter where first 3 Super Categories and all related sub-categories are blocked.
4. Select Policies and create a policy that uses that web filter you just created in step 3
5. Select the Organization Units tab and select the GSuite Organization units onto which you want to enforce CIPA compliant policy created in step 4 and then select 'Save' at the bottom of the page.



sales@blocksi.net
228 Hamilton Avenue (3rd floor), Palo Alto, California 94301
1 877 693 4822

BLOCKSI




Once these categories are saved, this Organization units will now be CIPA compliant. The base requirement for CIPA is to prevent exposure to minors of adult, violence, and inappropriate content. Blocksi Manager Education Everywhere filters are now protecting HTTP and HTTPS access to these sites for the selected groups. In addition to applying these base policies, organizations can expand security by filtering Youtube, specific website (black/white list), as well as using Blocksi rich and enhanced insight analytics to detect violation attempts.

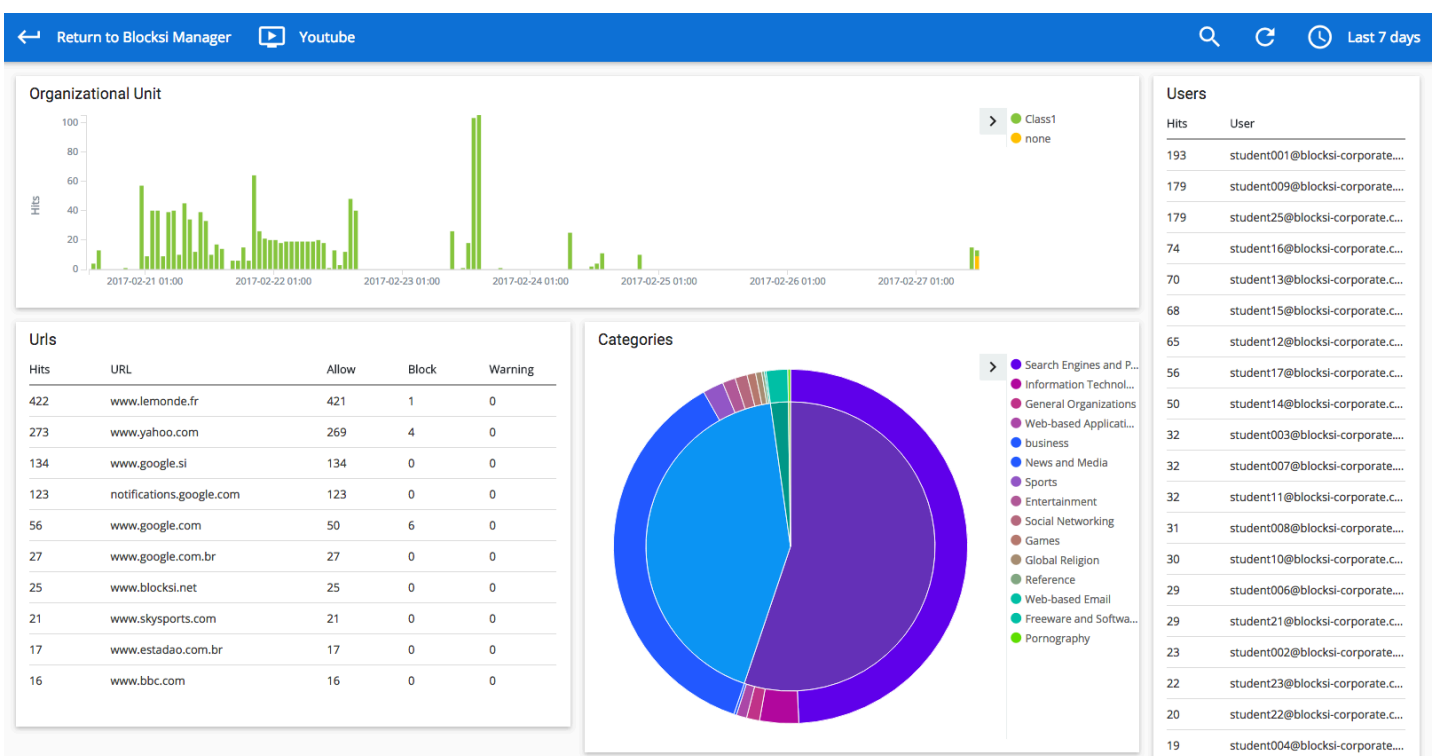


sales@blocksi.net
228 Hamilton Avenue (3rd floor), Palo Alto, California 94301
1 877 693 4822

BLOCKSI

# Blocksi Manager Education Everywhere Analytics and Insights per GSuite user.

The BMEE Analytics and Insight per GSuite user and per OU changes how we approach user-activity reporting and threat mitigation by addressing with whom and where your chromebooks or chrome clients are communicating with, wherever these devices are located, in campus or off campus.. By tapping exclusive features such as Geofencing and Blocksi content analysis per user, to identify threats and misbehaviors violating the school internet policies and lurking in the background. To access Analytics from the administrator dashboard, click Insights and you will land on the live activity analytics dashboard that will give you analytics at the user level regardless the network home or at school it has used his chromebook on.




blocksi.net

sales@blocksi.net
228 Hamilton Avenue (3rd floor), Palo Alto, California 94301
1 877 693 4822