Children’s Internet Protection Act (CIPA)

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.

Internet Content Filtering

Cisco Umbrella is a cloud-native platform that delivers the most secure, reliable, and fastest internet experience to more than 100 million users daily. Umbrella unifies firewall, secure web gateway, DNS-layer security, cloud access security broker (CASB), and threat intelligence solutions into a single platform to help businesses of all sizes secure their network. As more organizations embrace direct internet access, Umbrella makes it easy to extend protection to roaming users and branch offices.

cisco
Cisco Umbrella
First line of defense against internet threats
Learn
Intelligence to see attacks before they launch
See
Visibility to protect access everywhere
Block
Stop threats before connections are made

Google for Education

Built-in protections
User data is safeguarded with Gmail encryption and identity and access management.

Strong compliance
Google’s data protection practices comply with rigorous privacy and security requirements, and they’re audited regularly by third-party organizations.

No ads
There are no ads in Google Workspace for Education Core Services, and core service data is not used for advertising purposes. Also in Additional Services, K-12 (primary and secondary school) students’ personal information is not used for ad targeting.

Data transparency
Schools own their data — it’s our responsibility to keep it secure. Google operates its own secure servers and platform services, and makes it easy for admins to manage data security.

GoGuardian

Filtering and Monitoring
Manage filtering policies across all users, regardless of device type, operating system, or browser—from one interface.

Strong compliance
See student work in real time to quickly identify those who are off task or struggling, and those who are ready to move on. Easily recognize when a student strays from assigned material.

Teachers Interact with Student Screens
Open tabs to helpful resources, close irrelevant tabs, and annotate on a student’s screen to guide them towards purposeful content and help them maintain focus.

Beacon
Analyzes students' browsing behavior to alert people concerned of students at risk of suicide or self-harm

Internet Safety Policy (IJNDB)
Acceptable Use Policy

The **acceptable use policy** (AUP) is a set of rules applied by the owner of a network that restrict the ways in which the network, may be used and sets guidelines as to how it should be used.

FSD3's AUP :

District Rights and Responsibilities

- Monitor network and online activities
- Create/remove network user accounts
- Provide internal and external controls

Acceptable Use

- All use of the internet must be in support of educational objectives consistent with the mission and objectives of FSD3.
- Users of District technology resources have no reasonable expectation of privacy.

Unacceptable Use

- Any use of the network for commercial or for-profit purposes is prohibited.
- Malicious use of the network to develop programs that harass, bully or intimidate other users.
- Use of the network for any unlawful purpose is prohibited.
- Use of profanity, obscenity, threats, racist terms, libelous or defamatory language or other language that may be offensive or obscene to another user is prohibited.