Business & Non-instructional Operations

INTERNET FILTERING AND SAFETY

PURPOSE

The Board recognizes the importance of providing students with positive, productive educational experiences through the District's Internet services in addition to the District's Board Policy 4040, *Employee Use of Technology*, Board Policy 6163.5, *Student Use of Technology and Internet Safety* and Administrative Regulation 4040, *Employee Acceptable Use of Technology* and Administrative Regulation 6163.5, *Student Acceptable Use of Technology.*

To the extent practical, the Board directs the Superintendent or designee to:

- Prevent users from accessing or transmitting inappropriate material over the District computer network;
- Prevent unauthorized access and other unlawful online activity;
- Protect against damaging and costly legal liabilities due to exposure to inappropriate or offensive web content;
- Secure confidential information against spyware, phishing agents, and peer-to-peer transfers;
- Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
- Comply with federal and state laws.

To the extent practical, technology protection measures (or "Internet filters") shall be used on all District computers to control, block, or filter Internet, or other forms of electronic communications, access to:

- Bandwidth-intensive sites;
- Obscene material;
- Child pornography;
- Material deemed harmful to minors; or
- Other information that is determined to be in violation of District policies and the operation of such measures is enforced.

DEFINITIONS

Internet Filtering

Internet filtering refers only to web-based transmissions received through a web browser via the hypertext transfer protocol (HTTP). It does not refer to email, file transfers, instant messaging, or other material transferred over the Internet, even if such transfers involve web browsing software.

Federal Children's Internet Protection Act (CIPA)

CIPA requires schools and libraries receiving the federal E-Rate fund to limit children's access to the Internet in an attempt to prevent online access to pictures and sites that are obscene, contain child pornography, or are harmful to minors. Schools and libraries must certify that they have the appropriate filtering technology in place in order to receive discounts on computers and computer access from the government.

INTERNET FILTERING AND SAFETY

Filtering Implementation
It is necessary that the District have a networking team responsible for implementing the Internet Filtering and Safety administrative regulation. There will be at least one school technology manager who is a member of this team.

Filtering Profile or Profile
The Internet filtering technology chosen allows the District to customize the categories of websites to block or remain unblocked. A profile is the list of categories chosen to be blocked by the District.

Filter Management
The primary activity related to filter management is updating material to be blocked or unblocked. Automatic nightly downloads update the master library, and the District networking team has the ability to manually block or unblock websites.

FILTERING STANDARDS

The Internet filtering technology chosen by the District offers schools and libraries total CIPA-compliant Internet filtering, Internet monitoring, and reporting solutions. Categories blocked by the District's global profile include, but are not limited to:

1. Abortion
2. Adware
3. Alcohol/Tobacco/ Marijuana/Vaping
4. Child Pornography/ Child Abuse
5. Criminal Skills
6. Cults
7. Dating/Personals
8. Domain Landing
9. Dubious/Unsavory
10. Explicit Art
11. Free Hosts
12. Gambling
13. Games
14. Gore
15. Hacking
16. Hate and Discrimination
17. Illegal Drugs
18. Internet Radio
19. Image Server/ Image Search Engines
20. Intimate Apparel/ Swimwear
21. Intolerance
22. Invalid Web Pages
23. Malicious Code/Virus
24. Music/Audio
25. Online Communities
26. Obscene/Tasteless
27. Occult
28. Paranormal
29. Peer-to-Peer (P2P) File Sharing
30. Phishing
31. Piracy
32. Pornography/ Adult Content
33. R-rated Content
34. School Cheating
35. Shopping
36. Social Networking
37. Spyware
38. Streaming Media
39. Terrorist/Militant/ Extremist
40. Violence
41. Weapons
42. Web Blogs/Vlogs/ Personal Pages
43. Web-based Proxies/ Anonymizers

INTERNET FILTERING AND SAFETY

Minimum Filtering

The three categories necessary to minimally comply with Federal Children's Internet Protection Act (CIPA) requirements are blocked in the District's global profile:

1. Obscene/Tasteless
2. Pornography
3. Web-Based Proxies

Customized Filtering

In addition to the minimum and standard filtering in place, additional District customized categories provided are:

1. CUSD Allowed (District ruled exceptions)
2. CUSD Blocked (District ruled exceptions)

PROCEDURES

Request to Block Websites

1. Teachers, District staff, and administrators with filtering concerns should submit a request through myCUSD to the District networking team, which will review the details of the request. Please provide the exact URL in question and request a review with substantiation. The networking team will evaluate the request to block the site and give a response on whether it will be blocked or not within five business days.

2. If the requester disagrees with the decision, they may have it reviewed by an administrator or manager. The request for an appeal should be submitted to the District networking team, who will share such details with the network manager. Please include a copy of the response in question along with additional substantiation. The networking team will collaborate, and a decision will be made within five business days.

Request to Unblock Websites

1. Teachers, District staff, and administrators with filtering concerns should submit a request through myCUSD to the District networking team, who will review the details. Please provide the exact URL in question and request a review with substantiation. The networking team will evaluate the request to unblock the site and give a response on whether it will be unblocked or not within five business days.

2. If the requester does not agree with the decision, they may have it reviewed by a network manager. The request for an appeal should be submitted to the District network manager, who will share such details with the networking team. Please include a copy of the response in question along with additional substantiation. The networking team will collaborate, and a decision will be made within five business days.

Business & Non-instructional Operations

INTERNET FILTERING AND SAFETY

Authorized User Override Accounts

Only District Administrators may formally request an *Authorized User Override Account* to bypass the filter for conducting research or activities related to the discharge of their official responsibilities, provided this does not include activities that violate any provision of District policies, regulations, or procedures.

The request for such an account should be submitted to the District networking team, who will share the request with the network manager. Please include a list of the website(s) and respective Internet address(s) you require access to, and why access is necessary to discharge your official responsibilities.

A decision will be made within five business days, and if the outcome is favorable, the account details will be forwarded to the applicant via email. A similar timeline and advisory method will apply if the request is denied.

If an administrator believes an override account is being misused or the password has been compromised, they should report the matter immediately to the District webmaster.

Monitoring of Online Activities

The District's computer network manager and District networking team may monitor to ensure that the online activities of staff and students are consistent with the District's Board Policy 4040, *Employee Use of Technology*, Board Policy 6163.5, *Student Use of Technology and Internet Safety* and Administrative Regulation 4040, *Employee Acceptable Use of Technology* and Administrative Regulation 6163.5, *Student Acceptable Use of Technology* and this regulation.

ADDITIONAL INFORMATION

Users with questions about blocking/unblocking sites and local acceptable use/Internet filtering policies are encouraged to contact the District's network manager, who will share such details with the networking team, if necessary.

Approved: August 2009
Revised: July 22, 2025