LOS ANGELES UNIFIED SCHOOL DISTRICT
POLICY BULLETIN

TITLE: Web Content Filtering Policy

NUMBER: BUL- 5242.0

ISSUER: Ronald Chandler
Chief Information Officer

DATE: August 20, 2010

ROUTING
All Employees
All Locations

POLICY: The District is required to provide a safe learning environment for Internet access to all students at all locations.

MAJOR CHANGES: This is a new District policy.

BACKGROUND: The Children's Internet Protection Act (CIPA) is a federal law enacted in 2001 "to address concerns about access to offensive content over the Internet on school and library computers." Because many of the District's network projects are subsidized by the Federal E-rate program, the District is required to certify our compliance with CIPA.

CIPA requires the District to take measures to block access to web sites that are (a) obscene, (b) child pornography, or (c) harmful to minors. The District has adopted the Internet safety policy and must implement a solution that inspects web content and filters or blocks any web site meeting the criteria described above.

GUIDELINES: In order to comply with CIPA, the following defines sites that are blocked and the reasons.

Categories of Blocked Web Sites	Reason
Any web sites containing, or providing access to, **adult**, **pornographic**, **violent**, **racist**, or **hateful** content are deemed inappropriate for children and are blocked. The message "**Blocked by URL Filter Database**" appears when attempting to access any site meeting this criterion.	CIPA
Any site providing anonymous use of direct electronic communication such as **e-mail**, **chat rooms**, and **instant messaging**,	CIPA and District Policy
Web sites providing **games** are not considered harmful to minors, but are blocked during schools hours (7:00 AM to 3:00 PM) to limit distractions to the learning environment. "**Blocked During School Hours**" will display if an attempt is made to access any game site.	District Policy

Web sites that provide information that can be used for **hacking** or **filter avoidance** (**web proxies**) are blocked as these sites are deemed detrimental to the proper operation of the District's network.	District policy
Web sites that provide **peer-to-peer file sharing** services like Kazaa and Napster are considered an inappropriate use of network resources and are blocked.	District policy

There are millions of web sites and thousands added every day, so it is possible for web sites to be incorrectly categorized. If you are denied access to a site you believe to be acceptable, or you are allowed to visit a site that meets any of the criteria listed above, open a ticket with the Service Desk by going to http://techsupport.lausd.net/ and clicking on "Open A Service Request On-Line." The ticket will be routed to a member of the security staff and you will be notified by e-mail when the ticket is assigned and completed.

Although not immediately available, staff may be able to access selected blocked sites by using their Single Sign-On (SSO) account. Certain job classifications, such as school principals, will be granted permission to selected social networking sites. An IT governance committee, comprised of school and non-instructional staff, are developing a list of criteria that will guide policy on which positions can override security protocols.

RELATED RESOURCES:

- BUL-999.4: *Acceptable Use Policy (AUP) for District Computer Systems*
- BUL-1077.1: *Information Protection Policy*
- BUL-1759.0: *Authorized Internet Service Provider (ISP) Connections to District Locations*
- BUL-5181.0: *Policy Regarding Internet Safety for Students*
- Bulletin K-24: *District Firewall Policy*

ASSISTANCE:

For assistance or further information contact Information Technology Divisions (ITD) Service Desk at (213) 241-5200. For questions regarding this policy, contact Gash Teshome, Coordinator of IT Security at (213) 241-0627.