From: Steve Dantinne
To: mbanks@vineland.org
CC: mgruccio@vineland.org
Date: Monday, April 05, 2010 6:02:36 AM
Subject: Letter from Ms. Bosco

Bosco Letter.jpg

Dr. Banks,
I received this letter from Ms. Bosco, a teacher from VHSNorth.
How do you want me to proceed?

S. Dantinne

To: Mr. Steve Dantinne
From: Ms. Eileen Bosco
CC: Mr. Theodore Peters
Dr. Maryann Banks
Mr. Louis Russo
Date: March 28, 2010
Re: Websites

Mr. Dantinne,

I am writing to you regarding an issue with websites that are being blocked within our district. Much to my dismay, many of the websites that contain information regarding the LGBT (Lesbian Gay Bisexual Transgender) Community and issues within the LGBT Community, are blocked. The browser states that these sites are being blocked for "Categorization LGBT".

I understand that many times the filter will block sites for things such as inappropriate content; however, the State of New Jersey does not view LGBT issues, as inappropriate. As the advisor for the Gay Straight Alliance, I use many of these resources as materials for our club. I find it appalling that sites such as the Gay and Lesbian Alliance Against Defamation (GLAAD) and Parents, Families & Friends of Lesbian and Gays (PFLAG) are blocked, but students and faculty can gain access to the Westboro Baptist Church (www.godhatesfags.com). I have also found that we have access to the Klu Klux Klan homepage and Stormfront (an antisemetic white power site)

As a gay woman, I am offended and disturbed that the above information is true. I am requesting that someone review why these sites are being blocked and why in a district that promotes teaching tolerance I have to make this request. I would welcome the opportunity to meet with you and administration to discuss ways in which we can work together to make sure we represent all portions of school community.

I look forward to hearing from you.

Subject: Please unblock the Category LGTB for Elaine Bosco
From: Steve Dantinne <sdantinne@vineland.org>
Date: Wed, 14 Apr 2010 10:13:15 -0400
To: Jason Trzeciak <jtrzeciak@vineland.org>
CC: ebosco@vineland.org, "Dr. Banks" <mbanks@vineland.org>, Mary Gruccio <mgruccio@vineland.org>

Jason,

Please unblock the Category LGTB for Elaine Bosco

Steve

Ross Stanger

From: Ross Stanger [rstanger@vineland.org]
Sent: Thursday, February 17, 2011 4:26 PM
To: 'Steve Dantinne'; 'Mary Gruccio'
Subject: USII curriculum

Hi Steve and Mary.

I checked the USII curriculum and believe that the issue of the gay rights movement, as well as other reform movements, could easily be part of the curriculum. Frankly, it probably should have explicitly been mentioned as a reform movement of the late 60s and 70s. Here are the references from it which, I believe, support that assertion.

11-4.18 recognize and understand elements of the counter-culture movement. (6.2, 6.4)
11-4.19 examine the cultural changes reflected in the art, music and lifestyles of the 1960s. (6.4)

11-6.15 identify significant Congressional Acts and Supreme Court Cases since 1980. (6.2, 6.4)

11-6.16 examine the cultural changes reflected in the art, music and lifestyles since 1980. (6.4)

Here is a 2009 content standard that also supports this type of project or study.

D. History, Culture, and Perspectives	6.3.12.D.1	Analyze current laws involving individual rights and national se might be applied to a current case study that cites a violation of a

Times as Bob Dylan wrote are 'a changing.'

I am also copying info related to the history of gay rights which leads me to believe we should, **at minimum**, provide access for every teachers. However, because the history of the gay rights movement, feminist movement, and the black civil rights movements are so closely aligned, **it is my recommendation that we provide access to students and teachers. I can easily see a comparison of the three or the strategies used by the leaders as a viable project, especially in light of the recent repeal of 'don't ask don't tell'. For this reason I personally think granting access to students is the correct action.**

"Inspired by the African American Civil Rights Movement, homosexuals in America began to organize themselves and to fight for the equality and the justice they did not have yet. With the rise of gay rights activists, gay-rights opponents appeared, and the issue about homosexuals' rights turned into a controversial, legal battle, which today is still fought with neither party entirely winning.

By taking a close look at the history of gay rights, common prejudices against homosexuals, and the common arguments used on both sides of this topic without the emotional heat and biases, which is often linked with this controversial topic, one is able to think critically and approach the issue of homosexuality in a more reasonable way.

Homosexuals are defined as people who are sexually attracted by other persons of the same sex. The words "gays" or "gay people" are also common terms used instead of "homosexuals", whereas "lesbians" are only used to describe female homosexuals. These fundamental definitions of homosexuals already indicate that this minority group is evenly distributed throughout the entire society. Homosexuals can be both men and women. They exist in all classes, social groups, races, positions, and countries, regardless of their age or origin. As far as historians can trace back the past, homosexuals have always been in existence, including Julius Caesar, Plato, and Alexander the Great (Sloan 1).

History has also shown that gay people have always been discriminated against. Not only were gay people denied of equal treatment in court ("de jure"), but they also have been victims of violence and harassment in our own society on the base of their sexual orientation ("de facto"). Homosexuality was labeled a felony crime in the past, existing "Sodomy Laws" which prohibit oral and anal sexual intercourse, even between consenting adults, were primarily used to target homosexuals, and the current federal government denies openly gays employment to federal institutions like the CIA, FBI, the army -- nation's biggest employer in the United States -- or the National Security Agency. The government even regularly removes openly gay officials from public positions, and so do a lot of other employers in the private sector (Mohr 6).

In individual cases, homosexuals are often harassed, insulted, kicked, punched, and thrown at by fellow classmates, coworkers, and even family members just for being gay. These discriminations base on prejudices and stereotypes that society has of the gay community.

Among the most common stereotypes are those which carry fear and ignorance. Gays are said to be "child molesters" and "sex-crazed maniacs". They are considered extremely "immoral" because they do not follow social customs, "unnatural" because homosexuality violates the basic functions of genitals and contradicts the nature.

Religious leaders reason that Jesus asks the mankind in the Bible "to go out and have children." Since homosexuals are not able to reproduce children, homosexuality is, therefore, from their prospective an act of sin.

Gayness is considered by opponents a voluntary "act" and "behavior", which a person can act on. Some opponents go that far that, since homosexuality is from their point of view a matter of choice, their sexual practices are "crimes" which make homosexuals criminals.

On the other hand, gays defend themselves by arguing that homosexuality is a characteristic with which they are attached in the early childhood or even with birth. Gays do not have a choice over their homosexuality as heterosexuals do not have a choice over their heterosexuality. Hence, gayness is a condition over which they do not have, just as no one has control over his or her ethnic race, origin, outer appearance, or the class they he or she is born in. In addition, empirical research on adult sexual orientation and molestation of children has shown that gay men are not more likely to molest children than heterosexual men.

Based on this argumentation, homosexuals urged the government to ban discrimination of people on the basis of their sexual preference. However, up until the decades after the Second World War, in which Hitler did not only murdered Jews, but also homosexuals, there has been no powerful and effective gay rights movement. The reason for the ineffectiveness of the first movements lies in the fact that the gay community represents a so-called "invisible minority", that is a minority which "due to the fear of public inacceptance and disadvantage (losing one's job/public humiliation) do not openly reveal themselves" (Mohr 84). Just like the demand for freedom by slaves in the past resulted in more discrimination by the slave-owners, homosexuals faced the same vicious circle.

Since homosexuals often compare themselves with other minority groups like the Jews or the African Americans, they were very inspired by the African American Civil Rights Movement by Dr. Martin Luther King, Jr. His ideas, concepts, and demands for equal protection were adopted by the gay community, and especially King's success is the key element for the sudden rise of the Gay Rights Movement only several years later.

Ross Stanger
Supervisor of Instruction
Social Studies, Art, LEAP, Media Specialists, A.P.
Vineland Public Schools
625 Plum Street
Vineland, NJ 08360
(856) 794-6700 ext. 2016
rstanger@vineland.org

Subject: RE: LGTB Web Sites
From: "Dr. Banks" <mbanks@vineland.org>
Date: Thu, 24 Feb 2011 08:19:06 -0500
To: "'Steve Dantinne'" <sdantinne@vineland.org>

Steve,
I am having the sites reviewed by boe attorney. Do not provide access until I approve.
Thanks.

-----Original Message-----
From: Steve Dantinne [mailto:sdantinne@vineland.org]
Sent: Thursday, February 24, 2011 8:16 AM
To: Rich Panas
Cc: mgruccio@vineland.org; mbanks@vineland.org; ebosco@vineland.org
Subject: Re: LGTB Web Sites

Rich,
Send me the list.
Steve

On 2/24/2011 8:00 AM, Rich Panas wrote:

> Mary:
>
> I spoke with Eileen Bosco this morning regarding the LGTB web sites. She is going to meet with the students and come up with a list of appropriate web sites to be accessed during the school day.
>
> If you have any questions, please contact us. Thank you!
>
> Rich

Subject: Re: LGTB Web Sites
From: Steve Dantinne <sdantinne@vineland.org>
Date: Thu, 24 Feb 2011 08:23:30 -0500
To: "Dr. Banks" <mbanks@vineland.org>

Yes, I will wait for your direction
Steve

On 2/24/2011 8:19 AM, Dr. Banks wrote:

> Steve,
> I am having the sites reviewed by boe attorney. Do not provide access until I approve.
> Thanks.
>
> -----Original Message-----
> From: Steve Dantinne [mailto:sdantinne@vineland.org]
> Sent: Thursday, February 24, 2011 8:16 AM
> To: Rich Panas
> Cc: mgruccio@vineland.org; mbanks@vineland.org; ebosco@vineland.org
> Subject: Re: LGTB Web Sites
>
> Rich,
> Send me the list.
> Steve
>
> On 2/24/2011 8:00 AM, Rich Panas wrote:
>
>> Mary:
>>
>> I spoke with Eileen Bosco this morning regarding the LGTB web sites. She is going to meet with the students and come up with a list of appropriate web sites to be accessed during the school day.
>>
>> If you have any questions, please contact us. Thank you!
>>
>> Rich

Kevin Franchetta

From:	Steve Dantinne [sdantinne@vineland.org]
Sent:	Monday, March 28, 2011 8:00 AM
To:	Kfranchetta@vineland.org
Subject:	Here is the web filter we use for the district

Kevin,
Here is the web filter we use for the district.

http://www.bluecoat.com/products/webfilter

Other than specific requests to unblock sites which is determined by a principal conferring with the Supervisor of Technology, these categories and filters are the rule K-12 and adults.

Teachers have access to youtube

Administrators have access to all sites (facebook, myspace, etc.) other than pornography and adult in case they have to view/review students and staffs website postings which they have done outside of school.

Sites that threaten district network resources are also blocked for all.

Steve Dantinne

Kevin Franchetta

From: Steve Dantinne [sdantinne@vineland.org]
Sent: Monday, March 28, 2011 10:40 AM
To: Kfranchetta@vineland.org
Subject: Webfilter blacklist categories

Kevin, this is our blacklist (blocked) categories

Blacklist (manual entries)
Adult/Mature Content
Alternative Sexuality
Brokerage/Trading
Chat/Instant Messaging
Gambling
Games
Hacking
Illegal Drugs
Illegal/Questionable
LGBT
Nudity
Pay to Surf
Peer to Peer
Personals/Dating
Phishing
Pornography
Potentially Unwanted Programs
Proxy Avoidance
Real Estate
Remote Access Tools
Sex Education
Social Networking
Spyware Effects/Privacy Concerns
Spyware/Malware Sources
Suspicious

From: 997*Steve Dantinne [sdantinne@vineland.org]
Sent: Thursday, March 31, 2011 9:05 AM
To: jason@vineland.org
Cc: mgruccio@vineland.org; kfranchetta@vineland.org
Subject: Open Categorical Site

Jason, Effective immediately: open category LGBT on the Blue Coat filter for the two high school buildings, all staff and students.

S. Dantinne

Kevin Franchetta

From: Mary Gruccio [mgruccio@vineland.org]
Sent: Thursday, March 31, 2011 9:08 AM
To: 'Steve Dantinne'
Cc: 'Kevin Franchetta'; 'Ross Stanger'
Subject: web site request

Steve,

After review of the request to open LGBT website, it has been determined by Ross that the curriculum reflects the request. Therefore, please make the websites available at the VHS campus per Dr. Banks. Ross will be setting up a meeting with Mr. Panas, Ms. Bosco and the gentleman who made the request to inform them that we feel the request is valid and the website will be open for their use.

Kevin Franchetta

From: Jason Trzeciak [jtrzeciak@vineland.org]
Sent: Thursday, March 31, 2011 9:15 AM
To: '997*Steve Dantinne'
Cc: mgruccio@vineland.org; kfranchetta@vineland.org
Subject: RE: Open Categorical Site

Done.

From: 997*Steve Dantinne [mailto:sdantinne@vineland.org]
Sent: Thursday, March 31, 2011 9:05 AM
To: jason@vineland.org
Cc: mgruccio@vineland.org; kfranchetta@vineland.org
Subject: Open Categorical Site

Jason, Effective immediately: open category LGBT on the Blue Coat filter for the two high school buildings, all staff and students.

S. Dantinne

PURCHASE ORDER

VINELAND BOARD OF EDUCATION

VINELAND, NJ 08360

(856) 794-6700, EXT. 2248

IMPORTANT! This number should appear on all shipments and correspondence →

PURCHASE ORDER NO.
310857

DATE	LOCATION	DEPARTMENT	BUYER
01/28/11		TECHNOLOGY	119618

VENDOR:
INTEGRA BUSINESS CENTER INC 1813
INTEGRAONE
7248 TILGHMAN STE STE 120
ALLENTOWN PA 18106

BILL TO:
Vineland Board Of Education
Attn: Accounts Payable
17 West Landis Ave.
Vineland, NJ 08360-8122

INSIDE DELIVERY REQUIRED

TERMS	COL PPD	SHIP VIA

DELIVERY DATE	CONTRACT NO.

SHIP TO:
TECHNOLOGY
625 PLUM STREET
VINELAND, NJ 08360
ATTN: Steve Dantinne

ITEM NUMBER	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1	1	EA	1,583.59	1,583.59 119618
HSD3S1R-SG810-F Bluecoat REnewal Standard Support only 110-50000-0000-252-6000-00-517				
2	1	EA	6,334.35	6,334.35 119618
SL131R-SG8810-F Bluecoat REnewal Standart Support 24x7 L1-L1G Software Only 110-50000-0000-252-6000-00-517				
3	1	EA	615.59	615.59 119618
RNW-SVC-BCWF-500-999-1Y Renewal Service, Blue Coat WEbfilter 500-599 Users 110-50000-0000-252-6000-00-517				

Ok to pay

I certify that this purchase order has been executed consistent with the terms of N.J.A.C. 6A:10-2.1(f).

Signature

SUBTOTAL	8,533.53
FREIGHT	0.00
TOTAL	8,533.53

APPROVED FOR ISSUE Feb 10, 2011

BOARD SECRETARY'S SIGNATURE

NOTICE
The Board of Education is tax exempt
under Section 9(A): (1) of
Chapter 30 New Jersey Laws of 1966

ORIGINATOR'S FILE

Quote By:

integraONE
100 Corporate Center Drive
Camp Hill, PA 17011
Jason Reed
Phone (717) 614-4330 x 103
FAX (717) 828-1717

Prepared for:

Vineland Public School District
Steve Dantinne

sdantinne@vineland.org

Expires 30 days The information contained in this document is non-disclosure, and may be subject to change.

Quote	**VPS-11-1**
Total	**$8,533.53**
Date	**January 21, 2011**

To process your order as quickly as possible, please include the following on all purchase orders: Quote number, Billing and Shipping Address with contact name and phone number

				Bill Of Material			
Item#	**Product**	**Qty**	**Manufacturer**	**Product Description**	**Price**	**Discount**	**Total**
1	HSDSS1R-SG810-F	1	BlueCoat	Renewal, Same Day Ship, Standard Support,Hardware Only, *Prorated, SG810-F	$ 2,399.38	$ 1,583.59	$ 1,583.59
2	SL131R-SG810-F	1	BlueCoat	Renewal, Standard Support, 24x7 L1-L3 Software Only, *Prorated, SG810-F	$ 9,597.50	$ 6,334.35	$ 6,334.35
3	RNW-SVC-BCWF-500-999-1Y	1	BlueCoat	Renewal Service, Blue Coat WebFilter, 500-999 Users, *Prorated	$ 1,663.75	$ 615.59	$ 615.59
				Prices do not include delivery or any state, local taxes.		**TOTAL**	**$ 8,533.53**

***Service Renewal Proration Dates: 09/16/2010 01/31/2012**

All Sales are subject to Classic Networking's standard Terms and Conditions for purchase and support service. A copy of the standard terms is available upon request.

Quotation

Blue Coat

Quote #:2-5QVYDN **Version #: 1**

Address: 420 N Mary Avenue
Sunnyvale, CA 94085 USA
Phone: 408.220.2200 **Fax:** 408.220.2296
www.bluecoat.com
Federal Tax ID: 91-1715963
Date: 1/18/2011
Quote Contact: RITA.COHEN

Bill To: Westcon Group Incorporated
520 White Plains Road
TARRYTOWN, NY
United States

End User: Vineland
625 Plum Street
VINELAND, NJ
United States

Line #	Product	Serial #	Coverage Start Date	Coverage End Date	Period Covered	Blue Coat List Price	Qty/Users	Discount %	Extended Net Price
1	HSDSS1R-SG810-F	4306080421	09/16/2010	01/31/2012	16.5	$1,745.00	1	0%	$2,399.38
	Renewal, Same Day Ship, Standard Support,Hardware Only, 1 YR, SG810-F								
2	SL131R-SG810-F	4306080421	09/16/2010	01/31/2012	16.5	$6,980.00	1	0%	$9,597.50
	Renewal, Standard Support, 24x7 L1-L3 Software Only, 1 YR, SG810-F								
3	RNW-SVC-BCWF-500-999-1Y	QE7VP-X9Q66	09/16/2010	01/31/2012	16.5	$1,210.00	500	0%	$1,663.75
	Renewal Service, Blue Coat WebFilter, 500-999 Users, 1 Yr.								

Grand Total (USD): $13,660.63

With the issue of this quote any previous versions are no longer valid.
Please include the above Quote # and Version # on the renewal Purchase Order sent to Blue Coat Systems, Inc
Any questions regarding this quote should be directed to renewals-na@bluecoat.com, referencing the Quote # and Contact as above.
This quote does not include applicable taxes, freight, or customs/duty/tariff charges.These additional expenses will be added at the time of shipment.
Blue Coat Systems reserves the right to change or modify the quote if not fully processed by the expiry date shown. E&OE.

THIS QUOTE EXPIRES ON:

03/19/2011

PURCHASE ORDER

VINELAND BOARD OF EDUCATION

VINELAND, NJ 08360
(856) 794-6700 EXT. 2248

IMPORTANT! This number should appear on all shipments and correspondence → PURCHASE ORDER NO. 2802753

DATE	LOCATION	DEPARTMENT	BUYER
07/30/07		TECHNOLOGY	69895

VENDOR: DYNTEK SERVICES INC 16147
VERTEX A DYNTEK COMPANY
525 WEST LINCOLN DR
MARLTON NJ 08053

BILL TO:
Vineland Board Of Education
Attn.: Accounts Payable
17 West Landis Ave.
Vineland, NJ 08360-4515

INSIDE DELIVERY REQUIRED

TERMS	COL PPD	SHIP VIA

DELIVERY DATE	CONTRACT NO.
	12P F1232

SHIP TO:
TECHNOLOGY
625 PLUM STREET
VINELAND, NJ 08360
STEVE DANTINNE

ITEM NUMBER	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1	1	EA	1,995.00	1,995.00 69895
SG810A Blue Coat Proxy Appliance - includes 12x5 support card, NIC pass through card 110-50000-0000-252-6000-00-517				
2	1	EA	41,005.00	41,005.00 69895
SG810WF Blue Coat Content Filter - CIPA Compliant- 500 Web Filter Licenses- Promotional Offer. Quote DTK-VBOE BC-810F V2 State Contract #A81223 110-50000-0000-252-6000-00-517				

Principal's Signature

Asst. Superintendent's Signature

SUBTOTAL	43,000.00
FREIGHT	0.00
TOTAL	43,000.00

APPROVED FOR ISSUE

BOARD SECRETARY'S SIGNATURE

NOTICE
The Board of Education is tax exempt under Section 9(A): (1) of Chapter 30 New Jersey Laws of 1966

ORIGINATOR'S FILE

2,3,5

DYNTEK

Vertex, A DynTek Company
5 GreenTree Centre
Suite 310
525 Lincoln Drive West
Marlton, NJ 08053

Quotation

Vineland Public Schools
625 Plum Street
Vineland, NJ 08360
Attention: Steve Dantinne

Prepared By:
Fred Gibbons
856-834-1131
Fred.gibbons@dyntek.com
NJ State Contract #A81223

Date: 07/26/07
Quote: DTK-VBOE BC-810F V2

Blue Coat Proxy / Content Filter

Product Code	Description	Qty	Unit Price	Ext Price
	Product:			
SG810A	Blue Coat Proxy Appliance * Includes 12x5 support, SSL Card, NIC Pass Through Card	1	$1,995.00	$1,995.00
SG810WF	Blue Coat Content Filter * CIPA Compliant * 500 Web Filter Licenses - Promotional Offer	1	$41,005.00	$41,005.00
		DynTek Sell Price:		**$43,000.00**

Please forward your Purchase Order to DynTek at Fax: 856-834-1111, Attention: Order Processing

Blue Coat

Home Premium Content Login How to Buy BlueTouch Support Login Security Lab Sut

SOLUTIONS PRODUCTS RESOURCES PARTNERS SUPPORT & SERVICES COMPANY

Overview
ProxySG Appliances
Cloud Service
ProxyOne Appliance
Data Loss Prevention
PacketShaper Appliances
ProxyAV Appliances
ProxyRA Appliances
WebFilter
Reporter
Director
ProxyClient
IntelligenceCenter
PolicyCenter
CacheFlow Appliances
K9 Web Protection

Blue Coat WebFilter

Block malware and filter content according to strict policy controls

Overview Categories Resources

Contact Us

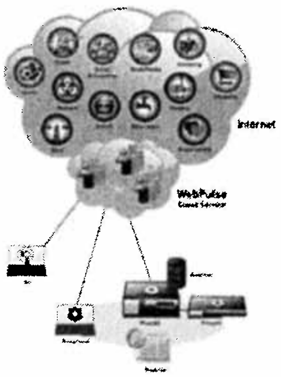
Find a rep →

Ask a question →

Locations →

As part of the Application Delivery Network (ADN), an infrastructure that provides complete application visibility, acceleration and security, Blue Coat WebFilter™ protects user productivity, blocks malware downloads and Web threats, and enables compliance.

WebFilter is continuously updated by the WebPulse community watch cloud defense that detects hidden malware and provides reputation and Web content analysis.



click to enlarge

WebFilter is 100% user driven for relevance creating an unmatched real-time Web content rating service. WebPulse uses Dynamic Link Analysis (DLA) to check popular Web sites for attack injections and search engine results for bait pages, both leading to Web threats via dynamic links.

WebPulse provides cloud intelligence to ProxySG Web gateways, and to ProxyClient and K9 Web Protection remote clients. WebFilter is the next generation of Web filtering, created by combining URL filtering and anti-malware technologies together into a collaborative cloud defense architecture.

Awareness & Response

WebFilter provides over 7 billion ratings per day for over 70 million users located in the largest enterprise and service provider networks around the world:

- WebPulse has eight operation centers to support cloud defense analysis of over 2 billion Web requests per week
- New Web content or links detected by Web gateways or remote clients are sent in real-time to the WebPulse cloud for DLA inspection where updates to the master WebFilter database provide immediate protection

- Blocks malware, Web threats, fake software updates, fake AV offers, phishing offers and botnets or keyloggers calling home
- Blocks only Web threats using DLA inspection, allowing users access to popular Web sites and avoiding over blocking
- Provides Web 2.0 filtering for mashed-up or customized web portals, blocking panels and dynamic content per policy settings
- Provides coverage in over 50 languages using proprietary machine analysis knowledge algorithms and human raters
- WebFilter integrates with Google malware feeds and other third party ratings for Web threats, phishing, scamware and content ratings

Protection Beyond the Web Gateway

ProxyClient provides enterprise remote users with WebFilter cloud protection requiring no downloads or update cycles for protection in any location or Web service:

- ClientManager provides custom filtering policies for ProxyClient, plus custom allow/deny URLs and categories
- K9 Web Protection extends the cloud protection of WebFilter to Internet parents and children for protection in any location at no charge
- Web gateways and clients are cloud connected for immediate protection, plus Web gateways can receive 5 minute updates for security categories, and 6 hour updates for all categories to improve Web gateway efficiency
- WebFilter is the only URL filtering solution to provide a real-time Web content rating service, a public accessible site review service, and a one day resolution process for ratings

Accuracy & Relevance

WebFilter is 100% user driven for Web content rating inputs from a broad and diverse user community without the need for Web crawlers or artificial analysis:

- For new customers, WebFilter quickly learns user Web habits with real-time feedback for relevance in new ratings
- WebFilter analyzes objectionable content, within image searches, cached content, and translation services for accurate ratings and compliance with its real-time rating service
- Extend WebFilter with custom categories, plus ProxySG supports up to four URL lists enabling global, regional and local filtering possibilities, including child protection
- WebFilter provides reputation ratings so policy controls can opt for inline threat analysis, or blocking downloads such as drive-by installers and executables from these sites
- Proxy Avoidance protection comes from WebFilter ratings plus ProxySG controls for user-agents and invalid SSL session controls

Dynamic Cloud Protection

WebPulse cloud analysis uses Dynamic Link Analysis (DLA) with four key elements to its architecture:

- A cloud connected user community of over 70M users that is broad and diverse
- Real-time input of any new Web links or content to the cloud analysis centers (Web gateway participation is optional, with on, off or passive mode settings)
- Immediate cloud analysis of new Web links using proactive machine analysis, a bank of anti-malware engines, Web correlations, human raters, active script analysis, and sandboxing
- WebFilter master cloud database updates to immediately protect all cloud connected Web gateways and clients with new ratings
- WebFilter is continuously updated by WebPulse cloud analysis using a DLA architecture that is unmatched by any other URL filtering solution
- WebPulse and DLA define the next generation of URL filtering for Web 2.0 content and dynamic links

Overview

ProxySG Appliances

Cloud Service

ProxyOne Appliance

Data Loss Prevention

PacketShaper Appliances

ProxyAV Appliances

ProxyRA Appliances

WebFilter

Reporter

Director

ProxyClient

IntelligenceCenter

PolicyCenter

CacheFlow Appliances

K9 Web Protection

Blue Coat WebFilter

Block malware and filter content according to strict policy controls

Overview **Categories** Resources

Contact Us

Find a rep →

Ask a question →

Locations →

The Blue Coat WebFilter database contains millions of Web site ratings representing billions of Web pages, covering more than 50 languages, and organized into 80 useful categories. If you feel your site has been improperly categorized, please visit: sitereview.bluecoat.com

- Abortion
- Adult/Mature Content
- Alcohol
- Alternative Sexuality/Lifestyles
- Alternative Spirituality/Belief
- Art/Culture
- Auctions
- Audio/Video Clips
- Blogs/Personal Pages
- Brokerage/Trading
- Business/Economy
- Charitable Organizations
- Chat/Instant Messaging
- Computers/Internet
- Content Servers
- Education
- Email
- Entertainment
- Extreme
- Financial Services
- For Kids
- Gambling

- Games
- Government/Legal
- Greeting Cards
- Hacking
- Health Sites
- Humor/Jokes
- Illegal Drugs
- Illegal/Questionable
- Internet Telephony
- Intimate Apparel/Swimsuit
- Job Search/Careers
- LGBT
- Media Sharing
- Military
- News/Media
- Newsgroups/Forums
- Non-viewable
- Nudity
- Online Meetings
- Online Storage
- Open/mixed Content
- Pay to Surf
- Peer-to-Peer (P2P)
- Personals/Dating
- Phishing
- Placeholders
- Political/Activist Groups
- Pornography
- Potentially Unwanted Software
- Proxy Avoidance
- Radio/Audio Streams
- Real Estate
- Reference
- Religion
- Remote Access Tools
- Restaurants/Dining/Food
- Search Engines/Portals
- Sex Education
- Shopping
- Social Networking
- Society/Daily Living
- Software Downloads
- Sports/Recreation

- Spyware Effects/Privacy Concerns
- Spyware/Malware Sources
- Suspicious
- Tobacco
- Translation
- Travel
- TV/Video Streams
- Uncategorized
- User-Defined
- Vehicles
- Violence/Hate/Racism
- Weapons
- Web Advertisements
- Web Applications
- Web Hosting

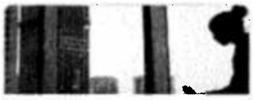
ProxySG also supports custom allow/deny URL lists as well as custom categories that apply to Web gateway deployments and remote user policies for ProxyClient. ProxySG supports up to four URL lists allowing organizations to user WebFilter with Internet Watch Foundation (IWF) URLs to block child pornography, regional URL lists and custom allow/deny URL lists.

Blue Coat

Home Premium Content Login How to Buy BlueTouch Support Login Security Lab Sut

SOLUTIONS PRODUCTS RESOURCES PARTNERS SUPPORT & SERVICES COMPANY

- Overview
- ProxySG Appliances
  - Full Proxy Edition
  - **Acceleration Edition**
  - Virtual Appliance
- Cloud Service
- ProxyOne Appliance
- Data Loss Prevention
- PacketShaper Appliances
- ProxyAV Appliances
- ProxyRA Appliances
- WebFilter
- Reporter
- Director
- ProxyClient
- IntelligenceCenter
- PolicyCenter
- CacheFlow Appliances
- K9 Web Protection



Virtual Classroom Training

Hands-on technical training from the convenience of your office.

Learn more and enroll →

Blue C eration Edition

Overview Featur **Specifications** Resources

For specification details, choose one of the ProxySG series below:

- Acceleration Edition -- ProxySG 9000 Series
- Acceleration Edition -- ProxySG 810 Series
- Acceleration Edition -- ProxySG 600 Series
- Acceleration Edition -- ProxySG 300 Series

ProxySG 9000 Series

	SG9000-5	SG9000-10	SG9000-20
License Capacity			
Concurrent Users	Unlimited	Unlimited	Unlimited
System			
Disk Drives	4x500GB SAS	8x500GB SAS	10x500GB SAS
RAM	4GB RAM	8GB RAM	16GB RAM
Onboard Ports	4 x 1000 Base-T: 1xMgmt, 1xAux, 1 bridged pair (WAN & LAN)		
Open Slots	3xPCI-E		
Optional NICs	4-port 1000 Base-T copper (2 bridges) 4-port 1000 Base-F Fiber (2 bridges) 2-port 10G Base-CX4 copper (1 bridge)		
Dimensions and Weight			
Enclosure	19" Rack-mountable		
Dimensions (L x W x H)	72.5cm X 42.7cm X 17.4cm (28.4in X 16.8in X 6.85in)		
Weight (maximum)	Approx. 40kg (90 lbs.)		
Operating Environment			
Power	AC power 100-240V, 50-60Hz, 9.0-4.5A		

Maximum Power	240 Watts	315 Watts	345 Watts
Thermal Rating	819 BTU/hour typical 3300 BTU/Hr max	1075 BTU/hour typical 3300 BTU/Hr max	1177 BTU/hour typical 3300 BTU/Hr max
Temperature	5°C to +40°C (41°F to 104°F)		
Humidity	Operating: 20% to 80% relative humidity, non-condensing; Storage: 10% to 90% relative humidity, non-condensing		
Altitude	Operating: Up to 3048 M (10,000 ft) Storage: Up to 12192 M (40,000 ft)		
Inrush Current:	2.60A@110V	3.30A@110V	3.30A@110V
Regulations			
Emissions	FCC/CISPR 22 Class A, EN 55022 / CISPR 22 Class A, IEC 61000-3-2 / EN 61000-3-2, IEC 61000-3-3 / EN 61000-3-3, CISPR 24 / EN 55024, VCCI Class A No.1706609, CE, BSMI, CCC, C-tick, KCC/RRL, Dictamen		
Safety	UL 60950-1, UL 94, IEC 60950-1/ EN 60950-1, CSA C22.2 No. 950 M95, TUV-GS, TUV-S, BSMI, CCC, KCC/RRL, Dictamen		
Standards	UL/CSA, TUV-GS, TUV-S, BSMI, C-tick, KCC, CCC, CE		
Certifications	Common Criteria EAL4+ in review, FIPS 140-2 anticipated		
Product Warranty Limited, non-transferable hardware warranty for a period of one (1) year from date of shipment. BlueTouch Support contracts available for 24/7 software support and options for hardware support.			

↑ back to top

ProxySG 810 Series

	SG810-10	SG810-20	SG810-25
License Capacity			
Concurrent Users	700	1000	Unlimited
System			
Disk Drives	2x300GB SCSI Ultra 320	4x300GB SCSI Ultra 320	4x300GB SCSI Ultra 320
RAM	4GB RAM	6GB RAM	6GB RAM
Network Interfaces	(2) integrated (on board) 10/100/1000 Base-T NICs 2x10/100/1000Base-T card (dual GigE with passthru) SSL card		
Optional Cards	None		
Optional NICs	2x10/100/1000Base-T card (dual GigE) 2x10/100/1000Base-T card (dual GigE with passthru) 2x1000Base-SX card (dual GigE Fibre) 4x10/100/1000Base-T card (quad GigE with passthru)		
Dimensions and Weight			
Enclosure	19" Rack-mountable		
Dimensions (L x W x H)	58cm x 44cm x 4.4cm (22.8in x 17.4in x 1.7in)		
Weight (maximum)	14.1kg(31lb)	14.5kg(32lb)	15.4kg(34lb)
Operating Environment			
Power	AC power 100-240V, 50-60Hz, 6.3-3.0A		
Maximum Power	375 Watts		
Thermal Rating	1280.25 BTU/Hr		
Temperature	5°C to 35°C (41°F to 95°F)		
Humidity	Less than 90% relative humidity, non-condensing		
Altitude	Up to 3048m (10,000ft)		
Regulations			

Emissions	FCC Class A, EN55022 Class A, VCCI Class A No.1706609, BSMI, CCC, C-tick, KCC
Safety	CSA C22.2 No. 950 M95, UL 60950 3rd Edition, EN60950, TUV-GS, TUV-S, CCC, BSMI
Standards	UL/CSA, TUV-S, BSMI, C-tick, CCC, CE
Certifications	ICSA, NIAP EAL 2, FIPS 140-2
Product Warranty Limited, non-transferable hardware warranty for a period of one (1) year from date of shipment. BlueTouch Support contracts available for 24/7 software support and options for hardware support.	

↑ back to top

ProxySG 600 Series

	SG600-10	SG600-20	SG600-35
License Capacity			
Concurrent Users	100	200	Unlimited
System			
Disk Drives	1x250GB SATA	2x250GB SATA	2x250GB SATA
RAM	4GB RAM	4GB RAM	4GB RAM
Network Interfaces	(2) integrated 1000 Base-T NICs with bypass, (1) integrated 1000 Base-T NIC for management, SSL card		
Optional NICs	4x1000Base-F card (GigE Fiber) 4x1000Base-T card (quad GigE with bypass)		
Dimensions and Weight			
Enclosure	19" Rack-mountable		
Dimensions (L x W x H)	37.5cm x 42.8cm x 4.3cm (14.76in x 16.83in x 1.7in)		
Weight (maximum)	8.72kg(19.2lb)		
Operating Environment			
Power	AC power 100-240V, 50-60Hz, 2.16-0.76A		
Maximum Power	150 Watts		
Thermal Rating	511.5 BTU/Hr		
Temperature	5°C to 40°C (41°F to 104°F) at sea level		
Humidity	20 to 80% relative humidity, non-condensing		
Altitude	Up to 3048m (10,000ft)		
Regulations			
Emissions	FCC Class A, EN55022 Class A, VCCI Class A, BSMI, CCC, C-tick, KCC		
Safety	UL 60950-1, EN60950-1, IEC 60950-1, CE Mark, TUV-GS, TUV-S, CCC, BSMI, GOST-R		
Standards	UL/CSA, TUV-S, BSMI, CCC, CE, GOST-R, Dictamine,C-tick, MIC		
Certifications	FIPS 140-2 (in process), NIAP EAL4+ (in process)		
Product Warranty Limited, non-transferable hardware warranty for a period of one (1) year from date of shipment. BlueTouch Support contracts available for 24/7 software support and options for hardware support.			

↑ back to top

ProxySG 300 Series

	SG300-5	SG300-10	SG300-25
License Capacity			
Concurrent Users	10	50	Unlimited
System			
Disk Drives	1x250GB SATA	1x250GB SATA	1x250GB SATA
RAM	2GB RAM	2GB RAM	4GB RAM
Network Interfaces	(2) integrated 1000 Base-T NICs with bypass (no SSL offload) (1) integrated 1000 Base-T NIC for management	(2) integrated 1000 Base-T NICs with bypass (SSL Card) (1) integrated 1000 Base-T NIC for management	
Dimensions and Weight			
Enclosure	Desk/rack mountable* (*standard rack shelf required).		
Dimensions (L x W x H)	26.4cm x 21.1cm x 4.14cm (10.4in x 8.3in x 1.63in)		
Weight (maximum)	2.6kg(5.7lb)		
Operating Environment			
Power	AC power 100-240V, 50-60Hz, 0.82-0.32A		
Maximum Power	65 Watts		
Thermal Rating	221 BTU/Hr		
Temperature	5°C to 40°C (41°F to 104°F) at sea level		
Humidity	20 to 80% relative humidity, non-condensing		
Altitude	Up to 3048m (10,000ft)		
Regulations			
Emissions	FCC Class A, EN55022 Class A, VCCI Class A, BSMI, CCC, C-tick, KCC		
Safety	UL 60950-1, EN60950-1, IEC 60950-1, CE Mark, TUV-GS, TUV-S, CCC, BSMI, GOST-R		
Standards	UL/CSA, TUV-S, BSMI, CCC, CE, GOST-R, Dictamine,C-tick, MIC		
Certifications	None		
Product Warranty			
Limited, non-transferable hardware warranty for a period of one (1) year from date of shipment. BlueTouch Support contracts available for 24/7 software support and options for hardware support.			

↑ back to top

Blue Coat

Home Premium Content Login How to Buy BlueTouch Support Login Security Lab Sut

SOLUTIONS PRODUCTS RESOURCES PARTNERS SUPPORT & SERVICES COMPANY

- Overview
- ProxySG Appliances
  - **Full Proxy Edition**
  - Acceleration Edition
  - Virtual Appliance
- Cloud Service
- ProxyOne Appliance
- Data Loss Prevention
- PacketShaper Appliances
- ProxyAV Appliances
- ProxyRA Appliances
- WebFilter
- Reporter
- Director
- ProxyClient
- IntelligenceCenter
- PolicyCenter
- CacheFlow Appliances
- K9 Web Protection

Blue Coat ProxySG Full Proxy Edition

Overview Features Specifications Resources

The Blue Coat Full Proxy Edition of ProxySG appliances are part of the Application Delivery Network (ADN) infrastructure that provides complete application visibility, acceleration and security. To support the Application Delivery Network, ProxySG delivers a scalable proxy platform architecture to secure Web communications and accelerate the delivery of business applications. ProxySG enables flexible policy controls over content, users, applications and protocols and is the choice of more than 80% of the Fortune® Global 500.

Layered Defenses Security Framework

ProxySG with WebPulse, the collaborative cloud defense uniting over 70M users for Web awareness to new Web content and threats, creates a hybrid design providing the best of on-premise controls with the collective intelligence of cloud service. ProxySG deployed with WebFilter automatically includes the WebPulse cloud service and ProxyClient for remote user protection, filtering and acceleration. ProxySG with ProxyAV enables the highest performing inline threat analysis, including SSL, with a choice of leading anti-malware engines. In addition, data loss prevention integration is securely enabled with S-ICAP or standard ICAP on ProxySG with certified DLP partners.

Unmatched Performance & Reliability

ProxySG innovations in new hardware platforms with multiple cores and the SGOS operating system with multithreading provide 1Gbps throughput for high availability deployments and scale 5X beyond the previous generation. SGOS is a micro kernel built for Web object processing, secure and small in design, it rarely needs attention or patches, and it runs year after year at performance levels beyond the competition. Health checks and monitoring provide administrator awareness, plus Director enables centralized device, license and policy management of ProxySG Web gateways.

Scalability and Lower TCO

The Blue Coat security framework scales in many ways, resulting in lower TCO for customers. The performance innovations require less hardware, rack space and power than alternative solutions. New defenses can be seamlessly added to the WebPulse cloud to scale the depth of protection. Expanding groups of remote users can accelerate office communications with ProxyClient plus be protected by WebPulse. And Reporter scales for

Application Delivery Assessment

Do you know what's running on your network?

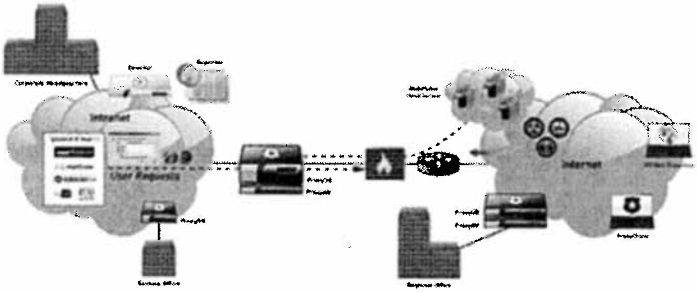
Find out now →

Virtual Classroom Training

Hands-on technical training from the convenience of your office.

Learn more and enroll →

visibility of all Web gateway and remote users with custom dashboards and reports on a single server with an included optimized database for up to 10B log lines.



Blue Coat provides a layered defense against Web 2.0 threats leveraging WebPulse cloud intelligence from over 70M users to protect the Web gateway and remote users. ProxySG provides unmatched policy flexibility, performance and reliability to secure networks and accelerate content

click to enlarge

Privacy Policy | EU Privacy Policy | Sitemap | US Government | Contact Us

Vineland Board of Education
Technology Plan
July 1, 2010 through June 30, 2013

III Technology Overview

B-2. District's Acceptable Use Policy

POLICY #2361.1 Acceptable Use of Computer Network/Computers and Resources

The Vineland Board of Education recognizes that as telecommunications and other new technologies shift the manner in which information is accessed, communicated and transferred that those changes will alter the nature of teaching, learning and tasks associated with the educational mission of the school district. Access to telecommunications will allow all members of the Vineland School District's educational community (administration, teachers, support staff, students, parents, board members) to explore databases, libraries, Internet sites, resource servers, and the like while exchanging information with individuals in the school district and throughout the world. The Vineland Board of Education supports access by members of the Vineland School District's educational community to information sources, but reserves the right to limit in school use to materials appropriate to educational purposes and the mission of the Vineland Public School District. The Vineland Board of Education directs the Superintendent or designee to effect training of all staff members in skills appropriate to analyzing and evaluating such resources as to appropriateness for educational purposes.

The Vineland Board of Education also recognizes that telecommunications will allow members of the Vineland School District's educational community (administration, teachers, support staff, students, parents, board members) access to information sources that have not been pre-screened by educators using the Vineland Board of Education approved standards. The Vineland Board of Education therefore adopts the following standards of conduct for the use of computer networks and declares unethical, unacceptable or illegal behavior as just cause for taking disciplinary action, limiting or revoking network access privileges and/or instituting legal action or taking any other appropriate action as deemed necessary.

The Vineland Board of Education provides access to computer network/computers for administrative and educational purposes only. The Vineland Board of Education retains the right to restrict or terminate access to any member(s) of the Vineland School District's educational community (administration, teachers, support staff, pupils, students, board members) to the computer network/computers at any time, for any reason. The Vineland Board of Education retains the right to have the Superintendent or designee monitor network activity, in any form necessary, to maintain the integrity of the network(s) and ensure its proper use.

The purpose the Internet is to support research and education in and among academic institutions in the world by providing access to unique resources and the opportunity for collaborative work. The use of Internet must be in support of education and research and consistent with the educational objectives of the Vineland Public Schools. Use of other organization's network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any U.S. or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material or material protected by trade secret. Use for commercial activities is generally not acceptable. Use for product advertisement or political lobbying is also prohibited. The use of the Internet is a privilege, not a right, and inappropriate use will result in cancellation of those privileges.

Standards for Use of Computer Networks
Any individual engaging in the following actions when using computer networks/computers shall be subject to discipline or legal action:

A. Using the computer network(s)/computers for illegal, inappropriate or obscene purposes, or in support of such activities. Illegal activities are defined as activities that violate federal, state, local laws and regulations. Inappropriate activities are defined as those that violate the intended use of the network. Obscene activities shall be defined as a violation of generally accepted social standards for use of publicly owned and operated communication vehicles.

B. Using the computer network(s)/computers to violate copyrights, institutional or third party copyrights, license agreements or other contracts.

C. Using the computer network(s) in a manner that:
1. Intentionally disrupts network traffic or crashes the network;
2. Degrades or disrupts equipment or system performance;
3. Uses the computing resources of the school district for commercial purposes, financial gain or fraud;
4. Steals data or other intellectual property;
5. Gains or seeks unauthorized access to the files of others or vandalizes the data of another user;
6. Network hardware/software monitoring, scanning, or "sniffing" for malicious code or intrusion is restricted to central office network management staff;
7. Gains or seeks unauthorized access to resources or entities;
8. Forges electronic mail messages or uses an account owned by others;
9. Invades privacy of others;
10. Posts anonymous messages;
11. Use of the network for personal and private business;
12. Any use of the network for product advertisement or political lobbying;
13. Network accounts are to be used only by the authorized owner of the account for the authorized purpose;
14. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users

on the network;
15. Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system;
16. Hate mail, harassment, discriminatory remarks and other antisocial behaviors;
17. Use of the network to access or process files dangerous to the integrity of the local area network or wide area network;
18. Use of network systems (data, video, voice) for soliciting or distributing information with the intent to harass, intimidate, or bully which can be described as Cyber Bullying;
19. Violating of any provision of individual privacy rights in accordance with FERPA (Family Educational Rights and Privacy Act) and the maintenance of confidential student and staff information;
20. Possesses any data which is a violation of this policy; and/or
21. Engages in other activities that do not advance the educational purposes for which computer network/computers are provided.

Internet Safety/Protection
The school district is in compliance with the Children's Internet Protection Act and has installed technology protection measures for all computers in the school district, including computers in media centers/libraries, that block and/or filter visual depictions that are obscene as defined in section 1460 of Title 18, United States Code; child pornography, as defined in section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, graphic image file or other visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

The school district will certify on an annual basis, that the schools, including media centers/libraries, in the district are in compliance with the Children's Internet Protection Act and the school district enforces the requirements of this policy.

This Policy also establishes Internet safety policy and procedures in the district as required in the Neighborhood Children's Internet Protection Act. This policy addresses access by minors to inappropriate matter on the Internet and World Wide Web; the safety and security of minors when using electronic mail and other forms of direct electronic communications; unauthorized access, including hacking and other unlawful activities by minors online; unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors.

Notwithstanding blocking and/or filtering the visual depictions prohibited in the Children's Internet Protection Act, the Vineland Board of Education shall determine other Internet material that is inappropriate for minors.

In compliance with yearly certification requirements of CIPA, the Vineland School District will disseminate the district's methods and policies regarding filtered Internet access to the educational community through the district's website, (www.vineland.org) email, and the district's educational access channel 13.

Security

Security on any computer system is a high priority, especially when the system involves many users. If a user feels they can identify a security problem on the Internet or the Vineland School District's network, the user must notify the Site Based Technology Coordinator (SBTC), Computer Technician, the Building Principal or the Supervisor of Technology. Do not demonstrate the problem to other users. Attempts to log on to the network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Cyber bullying

As per 2002 New Jersey Law, AB 1874, the state legislature finds and declares that : a safe and civil environment in school is necessary for students to learn and achieve high academic standards; harassment, intimidation or bullying, like other disruptive or violent behaviors, is conduct that disrupts both a student's ability to learn and a school's ability to educate its students in a safe environment.

In compliance with that law, usage and employment of network systems (data, video, or voice) to harass, intimidate, or bully which can be described as Cyber bullying, is unacceptable.

If a user feels they are the subject of Cyber Bullying, the user should notify the Site Based Technology Coordinator (SBTC), Computer Technician, the Building Principal or the Supervisor of Technology.

Violations

Individuals violating this policy shall be subject to the consequences as indicated in this document and other appropriate discipline, which includes but are not limited to:

1. Use of the network(s)/computers only under direct supervision;
2. Suspension of network privileges;
3. Revocation of network privileges;
4. Suspension of computer privileges;
5. Revocation of computer privileges;
6. Suspension from school (student);
7. Expulsion from school (student);
8. Reprimand, suspension and/or dismissal (staff members);
9. Legal action and /or referral to prosecuting authorities; and/or
10. Any other appropriate action that may be deemed necessary as determined by the Superintendent and approved by the Board of Education.

All employees shall be required to acknowledge receipt of this Policy 2361.1 and to execute an Acceptable Use of Computer Network/Computers and Resources Agreement pursuant to this Policy. Refusal to sign and acknowledge receipt of this form may, at the discretion of the District, be deemed insubordination.

N.J.S.A. 2A:38A-3
Federal Communications Commission: Children's Internet Protection Act.

Adopted: 12 November 1997
REVISED: 09 April 2003
REVISED: 17 November 2003
REVISED: 10 August 2005

Vineland Board of Education
Technology Plan
July 1, 2010 through June 30, 2013

III Technology Overview

B-3. District's Internet Safety Policy

The district's Internet safety policy addresses the following:

a) technology protection measures that protects against access through computers with Internet access to visual depictions by adults or minors that are

(I) obscene; or
(II) child pornography; or
(III) harmful to minors; and

b) process for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response, as required by the Protecting Children in the 21st Century Act.

POLICY #2361 INTERNET USE POLICY

Internet access is now available to students and teachers in the Vineland Public Schools. The Board of Education is pleased to bring this access to Vineland Public Schools and believes the Internet offers vast, diverse, and unique resources to both students and teachers. The Board's goal in providing this service to teachers and students is to promote educational excellence in schools by facilitating resource sharing, innovation, and communication.

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. Students and teachers have access to:

1. electronic mail communication with people all over the world.
2. information and news from NASA as well as the opportunity to correspond with the scientists at NASA and other research institutions.
3. public domain software and shareware of all types.
4. discussion groups on a plethora of topics ranging from Chinese culture to the environment to music to politics.
5. access to many University Library Catalogs, the Library of Congress and ERIC.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. Vineland Public Schools has taken precautions to restrict access to controversial materials. However, on a global network it is impossible to control all materials and an industrious user may discover controversial information. The Board firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the Vineland Public Schools.

Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. This policy is provided so that all are aware of the responsibilities each is about to acquire. In general this requires efficient, ethical and legal utilization of the network resources. If a Vineland Public Schools user violates any of these provisions, future access could possibly be denied.

Internet Terms and Conditions

1. Acceptable Use - The purpose of NSFNET, which is the backbone network to the Internet, is to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work. The use of Internet must be in support of education and research and consistent with the educational objectives of the Vineland Public Schools. Use of other organization's network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any U.S. or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret. Use for commercial activities is generally not acceptable. Use for product advertisement or political lobbying is also prohibited.

2. Privileges - The use of the Internet is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. Each student who has access to the Internet will be part of a discussion with a Vineland Public Schools faculty member pertaining to the proper use of the network. The system administrators will deem what is inappropriate use and their decision is final. Also, the system administrators may close an account at any time as required. The administration, faculty, and staff of Vineland Public Schools may request the system administrator to deny, revoke or suspend specific user accounts. No student account may be transferred by a student to another student nor used by another student.

3. Network Etiquette - Students are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

a. Be polite. Do not get abusive in your messages to others.

b. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.

c. Do not reveal your personal address or phone numbers or any other personal information of students or colleagues.

d. Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

e. Do not use the network in such a way that you would disrupt the use of the network by other users.

f. Do not play games or use the computer resources for other non-academic activities when others require the system for academic purposes.

g. Do not waste nor take supplies, such as paper, printer ribbons, and diskettes, that are provided by Vineland Public Schools in a computer lab.

h. All use of the Internet must be in support of education and research and consistent with the purposes of Vineland Public Schools. i. Any use of the network for commercial or for-profit purposes is prohibited.

j. Use of the network for personal and private business is prohibited.
k. Any use of the network for product advertisement or political lobbying is prohibited.
l. Network accounts are to be used only by the authorized owner of the account for the authorized purpose.
m. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the network.
n. All communications and information accessible via the network should be assumed to be private property.
o. No use of the network shall serve to disrupt the use of the network by others; hardware or software shall not be destroyed, modified, or abused in any way.
p. Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.
q. Hate mail, harassment, discriminatory remarks and other antisocial behaviors are prohibited on the network.
r. The illegal installation of copyrighted software for use on district computers is prohibited.
s. Use of the network to access or process pornographic material, inappropriate text files, or files dangerous to the integrity of the local area network is prohibited.
t. Any student use of Internet "live chat" capabilities will be directly supervised by an administrator, faculty or staff member.
u. Use of network systems (data, video, voice) for soliciting or distributing information with the intent to harass, intimidate, or bully which can be described as Cyber Bullying;
4. Vineland Public Schools makes no warranties of any kind, whether expressed of implied, for the service it is providing. Vineland Public Schools will not be responsible for any damages you suffer. This includes loss of data resulting from delays, nondeliveries, mis-deliveries, or service interruptions caused by its own negligence or user errors or omissions. Use of any information obtained via the Internet is at user's own risk. Vineland Public Schools specifically denies any responsibility for the accuracy or quality of information obtained through its services.

5. Security - Security on any computer system is a high priority, especially when the system involves many users. If a user feels they can identify a security problem on the Internet, the user must notify a teacher or other staff member or your System Coordinator. Do not demonstrate the problem to other users. Attempts to log on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to Internet.

6. Cyber bullying- As per 2002 New Jersey Law, AB 1874,"the state legislature finds and declares that: a safe and civil environment in school is necessary for students to learn and achieve high academic standards; harassment, intimidation or bullying, like other disruptive or violent behaviors, is conduct that disrupts both a student's ability to learn and a school's ability to educate its students in a safe environment".

In compliance with that law, usage and employment of network systems (data, video, or voice) to harass, intimidate, or bully which can be described as Cyber bullying, is unacceptable.

If a student feels they are the subject of Cyber Bullying, the student should notify a teacher or other school staff member immediately.

7. Vandalism - Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet, or any of the above listed agencies or other networks that are connected to the NSFNET Internet backbone. This includes, but not limited to, the uploading or creation of computer viruses.

8. The user should recognize that software is protected by copyrights laws; therefore, user will not make unauthorized copies of software found on school computers, either by copying them onto his/her own diskettes or onto other computers through electronic mail or bulletin boards; user will not give, lend, or sell copies of software to others unless user has the written permission of the copyright owner or the original software is clearly identified as shareware or in the public domain.

9. The user should recognize also that the work of all users is valuable; therefore, user will protect the privacy of each other's areas by not trying to learn their passwords; user will not copy, change, read, or use files in another user's area, without that user's prior permission; user will not attempt to gain unauthorized access to system programs or computer equipment' user will not use computer systems to disturb or harass other computer users by sending unwanted mail or by other means; and user will not download information onto the hard drives of any Vineland Public School computer for permanent storage.

10. Any user who does not comply with this policy will lose network privileges as determined by the building principal. Repeated or severe infractions of this policy may result in termination of access privileges permanently. Student infractions may result in appropriate disciplinary action in addition to suspension or termination of access privileges. Unauthorized use of the network, intentional deletion or damage to files and

date belonging to other users, or copyright violations may be termed theft as defined under New Jersey Revised Statutes.

11. All building principals shall obtain parent's and student's consent to these guidelines in the form of a written agreement.

Adopted: 11 June 1997
Revised: 12 October 2005

III Technology Overview

B-4. CIPA Public Hearing

A public presentation was offered on Wednesday March 24, 2010 at 5PM in the board of education room at 625 Plum Street, Vineland, NJ 08360 and also made available on Channel 9. There is also a web video presentation available as listed below.

Children's Internet Protection Act

- **CIPA -FCC Consumer Facts**
- **CIPA Presentation - Video, 6 minutes**
- **Blue Coat Web Filter -Control Access to Web Content and Block Web Threats**
- **Children's Internet Protection Act (CIPA) -State of NJ Dept. of Education Web**