Prince William County
PUBLIC SCHOOLS
Providing A World-Class Education

April 29, 2011

Via Electronic Mail

Rebecca K. Glenberg
rglenberg@acluva.org

RE: *FOIA Request of April 11, 2011*

Dear Mrs. Glenberg:

The Prince William County Schools (PWCS) Office of Equity and Compliance Office is in receipt of your email dated April 11, 2011, pertaining to the ACLU FOIA request. This letter and enclosed documents are responsive to that request. A response to each of your requests is outlined below.

1. *The district's use of internet filtering software to block websites that fall into the category of "LGBT," "Gay or Lesbian or Bisexual Interest," "Alternative Lifestyles," "Social Issues," or any similar category at high schools in the district;*

Enclosed please find PWCS Internet Content Filter Procedure which provides a list of blocked categories, a copy of Regulation 295-1, "Computer Systems and Network Services- PWCS Acceptable Use and Internet Safety Policy," and a copy of the Purchase Orders pertaining to Blue Coat.

2. *The district's use of internet filter software to block the following websites:*
Day of Silence: http://dayofsilence.org
The Trevor Project: http://thetrevorproject.org/
GSA Network: http://gsanetwork.org
Gay, Lesbian, Straight Education Network: http://glsen.org/
The It Gets Better Project: http://www.itgetsbetter.org

There are no documents responsive to this request. Under Va. Code § 2.2-3704.D, public bodies shall not be required to create a new record which does not already exist. Therefore, the Division must deny this request, pursuant to Va. Code § 2.2-3704.B.3.

3. *Any requests to block or unblock specific websites and the resolution of such requests;*

   The request above indicated that you were looking for documents in regards to “specific websites.” It was assumed you were referring to LGBT web sites. The documents related to LGBT web sites responsive to this request are enclosed.

   In the event you would like copies of requests to block or unblock *any* web sites, including those not pertaining to LGBT, it is estimated that the time it would take to access, duplicate, supply, and/or search for the requested records, is likely to well exceed $200.00. Before processing this request a deposit in the amount of $1,000 would be required.

4. *Which categories of websites were selected to be clocked pursuant to the default configuration of the internet filtering software (i.e. the configuration in place at the time the software was initially installed);*

   There are no documents responsive to this request. Under Va. Code § 2.2-3704.D, public bodies shall not be required to create a new record which does not already exist. Therefore, the Division must deny this request, pursuant to Va. Code § 2.2-3704.B.3.

5. *Who made the decision to activate the filter for "LGBT," "Gay or Lesbian or Bisexual Interest," "Alternative Lifestyles," "Social Issues," or any similar filter category, when the decision was made, and any communications concerning that decision.*

   There are no documents responsive to this request. Under Va. Code § 2.2-3704.D, public bodies shall not be required to create a new record which does not already exist. Therefore, the Division must deny this request, pursuant to Va. Code § 2.2-3704.B.3.

6. *The internet filtering provider(s)' knowledge that the filter for "LGBT," "Gay or Lesbian or Bisexual Interest, "Alternative Lifestyles," "Social Issues," or any similar filter category had been (or would be) enabled on the district's internet filtering software;*

   There are no documents responsive to this request. Under Va. Code § 2.2-3704.D, public bodies shall not be required to create a new record which does not already exist. Therefore, the Division must deny this request, pursuant to Va. Code § 2.2-3704.B.3.

7. *Communications between the internet filtering provider(s) and any representative or agent of Greenville County Schools concerning which categories of websites had been (or would be) blocked*

   There are no documents responsive to this request. Under Va. Code § 2.2-3704.D, public bodies shall not be required to create a new record which does not already exist. Therefore, the Division must deny this request, pursuant to Va. Code § 2.2-3704.B.3.

8. *Contracts and agreements, including service and maintenance agreements, between the internet filtering provider(s) and any representative or agent of Greenville County Schools.*

   There are no documents responsive to this request. Under Va. Code § 2.2-3704.D, public bodies shall not be required to create a new record which does not already exist. Therefore, the Division must deny this request, pursuant to Va. Code § 2.2-3704.B.3.

All documents that were responsive to your request are enclosed.

The costs incurred by the Division in locating, reviewing and copying the documents totals $2,217.09, calculated as follows:

Identifying, accessing, and reviewing requested records

Jim Hite	10 hours	$66.95/hr	$669.50
Jason Dasher	40 hours	$37.71/hr	$1508.40
Christi Hetrick	1 hour	$39.19/hr	$39.19
33 pages scanned			
TOTAL:			**$2,217.09**

In your FOIA request, you indicated, "If the costs of the copies is expected to exceed $50, please let me know the estimated cost before filling this request." We were unable to accurately predict the time and resources necessary to indentify, review and locate the documents responsive to your request. Since we were unable to notify you ahead of time, the decision was made to reduce the fees associated with the request to **$50.00.** Please make your payment for **$50.00** payable to the "Prince William County School Board." Mail to: PWCS, HR Attn: Christi Hetrick, P.O. Box 389, Manassas, VA 20108.

Very Truly Yours,

Christi Hetrick / KSA.

Christi Hetrick
Administrative Coordinator
Office of Equity and Compliance

Prince William County
PUBLIC SCHOOLS
Providing A World-Class Education

Internet Content Filter Procedure

Websites are filtered according to the web content filter list and a black list hosted locally on the proxy application firewall appliances. The blacklist is used for websites that may not be categorized yet but need to be filtered or do not fall under a defined category but have been reviewed and requested to be filtered.

Users are to submit requests for filtering/unfiltering of websites via the infosec-content heat ticketing system category. This was created so that Information Security and Instructional Technology could effectively process, save and track content filter inquiries as well as a centralized point to communicate with requestors. The ticketing system also gives ITS a filtering process so that Instructional Technology does not get requests that do not relate to actual AUP (Acceptable Use Policy) content filter verification but to other technology or protocol issues preventing websites from being accessed. The process is initiated by a end user opening up a heat ticket, Information Security then validates if the request is something that is technically a valid content filter request that needs Instructional Technology to evaluate against Virginia legal code § 22.1-70.2. Acceptable Internet use policies for public and private schools (http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+22.1-70.2), Federal CIPA law (Children's Internet Protection Act) and PWCS AUP 295-1 and then Information Security forwards it onto Instructional Technologies designated representative giving any technical perspectives on the site that might affect their decision. At this point Instructional Technology evaluates the request, responds to Information Security with their decision and Information Security filters/unfilters the website and updates the ticket with all pertinent information including communications between Information Security and Instructional Technology.

BlueCoat Web Content Filter Categories Enabled:
Abortion
Adult/Mature Content
Alcohol
Alternative Sexuality/Lifestyle
Chat/Instant Messaging
Extreme
Gambling
Games
Hacking
Humor/Jokes
Illegal Drugs
Illegal/Questionable
Intimate Apparel/Swimsuits
LGBT
Nudity
Peer-to-Peer (P2P)
Personals/Dating
Phishing
Placeholders
Pornography
Proxy Avoidance
Remote Access Tools
Social Networking
Spyware Effects/Privacy Concerns
Suspicious

Tobacco
__Violence/Hate/Racism
Category descriptions are explained in detail at the following website url:
http://sitereview.bluecoat.com/catdesc.jsp

Web page review website: Lists what a particular website is categorized at the present time:
http://sitereview.bluecoat.com/sitereview.jsp

All websites queried on bluecoat appliances go to bluecoat for review if they are not currently categorized. Those are normally categorized within 24-36 hours.

APPROVALS

Title	***Name***	***Request approved signature***	***Request denied signature***	***Date***
Instructional Technology Supervisor	Pat Donahue			
Instructional Technology Specialist Curriculum	Ginny Carrigan			
Information Technology Services Director	Jim Hite			
ITS Security Specialists	Jason Dasher			

Regulation 295-1
GENERAL SCHOOL ADMINISTRATION
May 27, 2009

GENERAL SCHOOL ADMINISTRATION

Computer Systems and Network Services - PWCS Acceptable Use and Internet Safety Policy

This regulation contains the Acceptable Use and Internet Safety Policy of the Prince William County Public Schools, as authorized in Policy 295, Standards for Use of Telecommunications and Internet Technologies. This governs the use of all Prince William County Public Schools (PWCS) local area networks, wired and wireless, wide area networks, the Internet/Intranet/Extranet-related systems, all PWCS Web sites, and all other similar networks. This policy also specifically applies to the use of PWCS computer equipment; software; operating systems; storage media; network accounts providing access to network services, such as email; Web browsing and file systems; as well as telecommunication technologies such as telephones, personal computers, cellular phones, Personal Digital Assistants (PDAs), facsimile machines, and all other wired or wireless telecommunication devices. To the extent this regulation can apply to other information and telecommunication technologies, it shall be interpreted to apply to them as well. This document supersedes all previous Acceptable Use policies and regulations for Prince William County Public Schools.

I. PWCS Instructional Philosophy

Prince William County Public Schools is committed to providing a World-Class education to meet the educational needs of our diverse student population. The instructional program in PWCS is implemented through a planned systematic approach which outlines the knowledge and skills to be taught in each subject and grade level.

Technology is a valuable tool that supports and enhances the PWCS instructional program by promoting problem solving, critical thinking, analytical, and decision making skills. Students and staff will access, process, and communicate information in a dynamic, integrated, and technological environment.

II. Expectation of Privacy

Employees and students have no expectation of privacy in their use of school computers or internet services, nor does the use of PWCS computers or related venues create an open or limited forum under the First Amendment to the federal or state constitutions. The Division retains the right to monitor all computer and Internet activity by employees and students, and any information or communications on PWCS computer systems and network services may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Use of PWCS computers, networks, and Internet systems is a privilege, not a right, and can be withdrawn by the Division at any time.

III. Acceptable Uses of PWCS Computer Systems and Network Services

It is the general policy that Prince William County Public Schools' computer systems and network services are provided for administrative, educational, communication, and research purposes consistent with the Division's educational mission, curriculum, and instructional goals. General rules and expectations for professional behavior and communication apply to use of the Division's computers, networks, and Internet services, as do those rules of student conduct set forth in the PWCS Code of Behavior. Acceptable uses of computer systems and network services include activities that support teaching and learning. Acceptable activities in support of this purpose include, but are not limited to, professional development, administrative communications, grant applications, new project announcements, and student product publishing.

A. Acceptable Use by Employees

Employees are to utilize the Division's computers, networks, and Internet services for school-related purposes and performance of job duties. Incidental personal use of school computers is permitted as long as such use does not interfere with the employee's job duties and performance, with system operations, or other system users. "Incidental personal use" is defined as use by an individual employee for occasional personal communications not occurring during instructional time, which use is not otherwise prohibited by this regulation.

B. Unacceptable Uses of PWCS Computer Systems and Network Services

Any infraction of the regulation will not be tolerated and PWCS will act quickly in correcting the issue if the Acceptable Use and Internet Safety Regulation is not followed. Any user found to have violated this regulation, Regulation 295-2, Web Site Development and Implementation, any other applicable School Board policy or regulation, or applicable provisions of the PWCS Code of Behavior are subject to disciplinary measures, up to and including, revocation of privileges; student discipline, up to and including expulsion; administrative action; employee discipline, up to and including dismissal; and criminal prosecution under applicable local, state and/or federal law.

C. Examples of Unacceptable Uses of PWCS Computer Systems and Network Services

The following is a non-inclusive list of examples of unacceptable actions or activities:

1. Any use that is illegal or in violation of other School Board policies or regulations;

2. Violating the rights to privacy of any student or employee;

3. Transmitting, downloading, storing, or printing files or messages (text, sound, still, or moving graphics, or any combination thereof) that are pornographic, or are obscene, as defined at Va. Code §18.2-372, or that use language, sounds, or imagery which is lewd or patently offensive (including "sexually explicit visual materials" as defined at Virginia Code §18.2-374.1), or degrades others (the administration invokes its discretionary rights to determine suitability in particular circumstances);

4. Transmitting, downloading, storing, viewing, or printing files or messages (text, sound, still or moving graphics, or any combination thereof) that are plainly offensive, lewd, vulgar, or are otherwise inconsistent with the curricula and educational mission of PWCS;

5. Harassment by computer, which includes transmitting any material or posting material on any Web site which is threatening to another person, or which is intended to coerce, intimidate, or harass; material intended to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature; or material threatening any illegal or immoral act, whether or not such material is transmitted to that third person;

6. The School Division has no legal responsibility to regulate or review off-campus Internet messages, statements, postings, or acts. However, PWCS reserves the right to discipline students or employees for actions taken off-campus, which would violate this Regulation if occurring on-site, if such actions adversely affect the safety, well-being, or performance of students while in school, on school buses, at school activities, or coming to and from school; if such actions threaten violence against another student or employee, if such actions violate local, state or federal law, or School Board policies or regulations or the Code of Behavior, or if such actions disrupt the learning environment, administration, or orderly conduct of the school. The Division may also take appropriate disciplinary measures, up to and including dismissal, for off-campus Internet activities which are inconsistent with the professional and ethical standards expected of PWCS employees as "role models" for PWCS students.

7. Copying and/or installing proprietary information, including software, in violation of software licensing agreements and applicable law;

8. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music or videos, and the installation of any copyrighted software for which PWCS or the end user does not have an active license is strictly prohibited;

9. Using the PWCS network or information contained on the network for personal financial gain, commercial, advertising, solicitation or business activity not on behalf of the Prince William County Public Schools, unless authorized under Regulation 923-1, Commercial Advertising, or any illegal activity;

10. Any use for a forum for communicating by email or any other medium with other school users or outside parties to solicit, proselytize, advocate, or communicate the views of an individual or non-school-sponsored organization; to solicit membership in or support of any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or non-profit. No employee shall knowingly provide names, email addresses, or other personal information to outside parties whose intent is to communicate with school employees, students and/or their families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable shall seek further guidance from their supervisor or the Director of Information Technology;

11. Sending mass emails to school users or outside parties for school or non-school purposes without the permission of an administrator;

12. Use of the PWCS network for political purposes, including any use requiring students to convey or deliver any materials that (a) advocate the election or defeat of any candidate for public office; (b) advocate the passage or defeat of any referendum question; or (c) advocate the passage or defeat of any matter pending before the School Board, the Prince William County Board of Supervisors, or the General Assembly of Virginia, or the Congress of the United States;

13. Any attempt to access unauthorized sites;

14. Any attempt to delete, erase or otherwise conceal any information stored on a school computer which violates these rules, or at any time after being advised by any administrator or supervisor to preserve any materials stored on a school computer;

15. Deliberately trying to degrade or disrupt system or network performance. Such acts will also be viewed as criminal activity under applicable state or federal law;

16. Transmitting or displaying messages promoting the sale of products/ services, except as provided in Regulation 923-1, Commercial Advertising.

17. Attempts to modify system facilities, downloading, installing, or transmitting viruses from email attachments or any other source, illegally obtaining extra resources, or attempting to subvert the restrictions associated with any computer system, computer account, network service, or personal computer protection software;

18. Writing down passwords and storing them anywhere accessible to others. Storing passwords in a file on ANY computer system (including PDAs or similar devices) without encryption;

19. Re-posting personal communications without the author's prior consent;

20. Transmitting unsolicited email messages or chain letters otherwise inconsistent with the curricula and educational mission of PWCS;

21. Personal use not related to educational or administrative purposes;

22. Fundraising or links to fundraising information on school/department Web sites or the Prince William County Public Schools Web page;

23. Sending PWCS proprietary and classified information to unauthorized persons, or posting this information outside of PWCS;

24. Distributing any school interior maps, floor plans, or written descriptions of interior floor plans on Web pages, camera locations, or other information which could compromise school security; and

25. Any content prohibited by Regulation 295-2, Web Site Development and Implementation.

IV. Areas of Responsibility

Employees, students, contractors, consultants, temporary employees of PWCS, including all personnel affiliated with third parties, volunteers in PWCS, and all other persons granted access to the PWCS network infrastructure must comply with, and are responsible for monitoring, enforcing, and reporting infractions of the PWCS Acceptable Use Policy.

- Central Office Managers (i.e., department supervisor or director) and Principals and other school-based administrators shall be responsible for ensuring that this Acceptable Use Policy and Regulation 925-2, Web Site Development and Implementation, and Commercial Advertising are followed. Administrators shall also monitor teacher use and supervise correct integration of technology into instruction.

- Web Managers within schools and central office departments shall also be responsible for ensuring that this Acceptable Use Policy and Regulations 923-1, Commercial Advertising, and 925-2, Web Site Development and Implementation, are followed.

- Teachers shall be responsible for guiding and monitoring student use of PWCS computer systems and network services and for providing Internet safety instruction to students.

- Students shall be responsible for adhering to the PWCS Acceptable Use and Internet Safety Policy and regulation and using PWCS computer systems and network services for assignments directly related to the curriculum.

- Parents shall be responsible for ensuring that their children adhere to the PWCS Acceptable Use Policy and regulation and use PWCS computer systems and network services for curriculum related assignments.

V. Security

A. Technology Protection Measures.

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act [Pub. L. No. 106554 and 47 USC 254(h)], blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, and the approval of the Director of Information Technology Services or designee, technology protection measures may be disabled or, in the case of minors, minimized for a bona fide research or other lawful purposes. Prince William County Public Schools Information Technology Services has implemented and maintains industry leading technologies to secure and provide safe Internet access to students and staff. Internet filtering complements Prince William County Public Schools' overall security strategy by use of a holistic approach in protecting students, employees, and network assets. PWCS filters and monitors Internet activity through technology protective measures used to block or filter Internet or other forms of electronic communications. Filtering shall be applied to all materials deemed inappropriate, in accordance with applicable laws. Subject to staff supervision, technology protection measures may be bypassed, or in the case of minors, minimized, for bona fide research or other lawful purposes. Authority for bypassing or modifying any technology protection measure must be obtained from the Director of Information Technology Services or his/her designated representative. It shall be the responsibility of all Prince William County Public Schools staff to supervise and monitor usage of the computer network and access to the Internet in accordance with applicable federal and state laws, guidelines, and regulations of the Virginia Department of Education, and School Board policies and regulations.

B. Employee and Student Data Privacy

These standards are structured to provide due diligence and compliance with applicable federal, state, and local laws and School Board policies and regulations for the protection of confidential information and privacy of student and employee information during the collection, transfer, storage, use, disclosure, and destruction of such information. To protect the privacy of employees and students, school system personnel are legally responsible for safeguarding the information collected about and from employees and students. The data should be kept intact from accidents, unauthorized access, theft, unauthorized changes, or unintentional release. Data handlers should understand what is considered appropriate and inappropriate access to data and use thereof. Changes, alterations, and distribution of data must be made only in authorized and acceptable ways. No encryption solution or file-sharing program may be utilized unless authorized and approved by the Director of Information Technology Services or designee.

The collection, use, and dissemination of personally identifiable student or employee information shall be strictly limited to bona fide educational or administrative purposes. Photos and names of students and staff are allowed on PWCS Web sites for the purpose of publicizing school activities or student achievement, but such information must be used with caution and in accordance with Regulation 790-3, Release of Directory Information, which gives students and their parents/guardians the right to opt out of public disclosure of their names, photos, and other student information. Information regarding individual students may only be used if it meets the definition of directory information contained in Regulation 790-3, and the student/parent/guardian has not opted out of such disclosure.

Social security numbers shall not be collected, disseminated, or disclosed, unless authorized by law. Personal information, such as names, job titles and descriptions, telephone and fax numbers, email and other addresses, may be collected and used internally for PWCS program/ seminar registration via the Internet or for participation in PWCS online programs or other legitimate PWCS purposes. Such information shall not be sold or shared with any external groups nor disclosed to any third party outside PWCS.

Files containing confidential or sensitive data may not be stored on removable media or mobile devices taken off PWCS property unless approved by the central office department manager /school principal and protected by an approved Information Technology Services encryption solution.

Individuals or companies under contract with PWCS may have access to information in the course of the service they provide to PWCS, but those entities are not permitted to use or re-disclose that information for unauthorized purposes and must sign a PWCS nondisclosure agreement prior to work being performed. No other entities are authorized to collect information through PWCS sites.

Risk Management must be notified immediately if sensitive or critical PWCS information is compromised or lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of PWCS information systems has taken place, or is suspected of taking place.

C. Access to PWCS Computer Systems and Network Services

Employees, students, and temporary employees of PWCS acknowledge their understanding of the Acceptable Use and Internet Safety Policy as a condition of receiving access to the computer system and network services. All employees will be reminded of the PWCS Acceptable Use expectations annually in employee newsletters (i.e. "Communicator," "the Leader"). Building administrators and/or department supervisors are responsible for reviewing the expectations with their staff.

D. User Accounts

All user-level, system-level, email, and application services must have a unique user identification. Users shall not allow others access to their account and are responsible for all activities performed with their account. Additionally, employee and students must not use the accounts of others to perform activities on PWCS information resources. It is the user's responsibility to ensure that this identification is not shared with others. Quarterly review of user accounts will be performed to purge outdated user accounts and to ensure compliance with this regulation.

- Use of generic and temporary network, application, and email accounts should not be deployed, unless approved by the Director of Information Technology Services or designated representatives.

- Users are not allowed more than one concurrent session and restricted access to PWCS business hours, unless authorized by the Director of Information Technology Services or designee.

- Employees are required to log out of computer sessions daily and prior to allowing another user access to a computer system in which they have an active session. Employees shall be responsible for any unauthorized use of a computer, network, or Internet system by any person or student who accesses the same because or while the employee has failed to log out as required.

- Laptop users are required to first login to the PWCS network via their network login account to create a local user account on the laptop system in order to provide logging and accountability of use while off site.

E. Authentication

Authentication is a method used to validate a user's authorization to access to a computer system or application. Users shall adhere to the following authentication procedures:

- Administrator and employee computer systems shall employ a PWCS-approved screen saver with "on resume password enable" required after 10 minutes.

- Users shall secure computer systems via the password protected screen saver when leaving computer systems unattended. This feature prevents unauthorized use of a computer system after a legitimate user has logged on, but is momentarily away from their computer. Public and student computers, such as those in the library or in labs, with no critical or sensitive information are excluded.

- Session time-outs of no more than five minutes are required on Web-based applications.

- Network connected computer systems and Web application services owned by PWCS shall have a warning banner on all access points and ensure that the banner is displayed whenever the system is turned on or at user login.

F. Passwords

A password is used in conjunction with a unique user identification in order to authenticate a user's right to access a computer system and application service. Passwords help protect against misuse by seeking to restrict use of PWCS systems and networks to authorized users. Authorized users are responsible for the security of their passwords and accounts. Passwords are considered secret and are not to be shared under any circumstance. Individual user passwords must never be embedded into an application or process. All user-level, system-level, email, and application service passwords must conform to these guidelines. Public computers, such as those in a library or in labs, with no critical or sensitive information, may be excluded on a case-by-case basis, as approved by the Director of Information Technology Services or designated representatives.

A password should be assigned to each unique user identification. Users are required to change passwords immediately upon first logging into the system and/or application.

If an account or password is known or suspected to have been lost, stolen, or disclosed, the user shall immediately report the incident to the Director of Information Technology Services or designated representatives, and change all passwords. Password requirements are located in Appendix III.

G. Email Accounts

Employees are assigned PWCS email accounts, to be utilized for educational purposes and official PWCS Division communication. Automated forwarding of email messages should be disabled unless authorized by the Director of Information Technology Services or designated representatives to prevent proprietary and classified information leaking to unauthorized persons or entities.

If students are assigned email accounts, a teacher must act as a sponsor. Sponsors are responsible for guiding and monitoring student communication and use of appropriate sections of the network and for assuring that students understand that misuse of the network will cause them to lose their accounts and/or face disciplinary action. When appropriate, sponsors will assume responsibility for teaching the students proper techniques and standards for participation; explain issues of privacy, copyright infringement, tool use, and network etiquette.

H. Hardware and Software

Software utilized by schools or individual departments that is intended for use on the PWCS network must be reviewed by the Information Technology Steering Committee prior to purchase or installation and approved by the Director of Information Technology Services or designee. The Department of Information Technology Services is responsible for obtaining and verifying the proper written authorization from information asset owners for granting access to system and/or application resources implemented on network connected computer systems. End users cannot install, run, or download software or modify configurations on network connected computer systems unless authorized by Information Technology Services. This stipulation is to ensure compliance with copyright laws, patch management, malware avoidance and overall infrastructure and computer system integrity. Installation of network connected computers, maintenance, repair, updates including hardware, and software, should be approved, directed, and completed by Information Technology Services.

The Division's malware/anti-virus software must be installed, enabled, and kept up-to-date on all network connected computer systems at all times. The malware/anti-virus software should be managed centrally and not configurable by end users. Weekly system scans should be performed on all computer systems. Malware infected computer systems must immediately be remediated or removed from the network until they are verified as malware-free.

As new vulnerabilities are discovered and software upgrades become available, computer systems must have the most recently available and appropriate software security patches, commensurate with the identified level of acceptable risk.

All systems (e.g., computers, monitors, printers) should be turned off at the end of the school/work day and on days when schools/offices are closed, with the exception of days/times established to allow for after-hours malware/anti-virus system scans and software/operating systems patch maintenance/upgrades (e.g., leaving computers on every Wednesday and Thursday evening). On occasion, schools/offices may be directed to leave computers on for special reasons/urgent matters concerning updates or data security issues that must be attended to immediately.

I. Remote Access

It is the responsibility of PWCS employees, contractors, vendors, and agents with remote access privileges to the PWCS network to ensure that their remote access connection is given the same consideration as the user's on-site connection to PWCS. All users in need of remote access to PWCS assets are required to use centrally administered tools and comply with the Information Technology Services Firewall Standards. Organizations or individuals who wish to implement non-standard remote access solutions to the PWCS network must obtain prior approval from the Director of Information Technology Services or designee. All computer systems that are connected to the PWCS internal network via remote access technologies must comply with all requirements of this regulation.

VI. Incident Response, Mitigation, Management, and Investigation

Incident response seeks to facilitate the discovery, management, mitigation, investigation, and awareness of computer system and network service related security incidents in a manner that complies with applicable laws, policies, and regulations. All identified security related incidences shall be reported to a site administrator or PWCS Risk Management Department immediately. PWCS Risk Management Department or the Director of Information Technology Services or designated representatives shall verify that an incident has occurred and determine what, if any, action needs to be taken (Appendix III). No user shall power off/on, disconnect, delete information from, or otherwise disturb any computer subject to seizure, unless under the direction of Risk Management or the Director of Information Technology Services or designated representatives.

VII. Preservation of Electronic Evidence

When the Division has notice of actual or anticipated litigation, it is required to preserve all evidence, including electronic evidence, related to such litigation. Employees who receive notice from PWCS of actual or threatened litigation (or become aware of such actual or threatened litigation from other sources) must preserve all such evidence and may not delete, alter, or otherwise disturb the integrity of any electronic evidence. This includes, but is not limited to, emails, files, folders, or any other electronic data or communications.

VIII. Internet Safety Instruction

Internet safety instruction is the responsibility of all instructional personnel. "NetSmartz", K-12 Internet safety curriculum provided by National Center for Missing & Exploited Children, and additional resources will be used with students at all grade levels.

The Internet Safety instructional plan can be found in Appendix III.

IX. Review Process

The Associate Superintendent for Communications and Technology Services (or designee) is responsible for implementing and monitoring this regulation and the Acceptable Use Policy.

The Associate Superintendent for Communications and Technology Services (or designee) is responsible for reviewing this regulation and the Acceptable Use Policy annually, with the assistance of the PWCS Department of Information Technology Services and Office of Instructional Technology. Every two years, the Division Superintendent will file an Acceptable Use Policy with the state that has been approved by the PWCS School Board.

APPENDIX I:

Resources

Contacts for Security Incidents

• Site administrator, principal, guidance counselor, or department supervisor	
• Risk Management and Security Services	703.791.7206
• Department of Information Technology Services	703.791.8722

Prince William County Public Schools Code of Behavior
http://pwcs.edu/studentservices/codeofbehavior.pdf

APPENDIX II

<u>Password Requirements</u>

- Minimum characters: 8
- Passwords must contain at least one letter, one numeral, and one special character
- No repeatable/consecutive characters
- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Contain numeric/special characters, such as 0-9, !@#$%^`&*()
- Password should not contain a word found in the (English) dictionary
- Expiration settings – at least once every six months
- None of a user's previous 3 passwords can be re-used
- Accounts should automatically lock after 3 consecutive failed login attempts for at least 30 minutes to sufficiently stop brute force password hacks with strong passwords enabled

APPENDIX III:

Internet Safety Instructional Plan

Schedule of Implementation

April, 2007	Research and develop Internet Safety program and implementation plan.
May, 2007	Review "NetSmartz" curriculum
Sept. - Dec., 2007	Determine concepts that will be taught at specific grade levels and develop any additional resources that are needed. Develop an online course to be accessed by teachers and administrators
Dec., 2007	Professional Development for Instructional Technology Resource Teachers Select schools to pilot curriculum
Jan. - Feb., 2008	Provide face to face and online professional development for teachers that will pilot the curriculum
Feb. - Apr., 2008	Pilot curriculum at selected schools
May - June, 2008	Evaluate pilot program
Aug., 2008	Report pilot results to Virginia DOE
Sept., 2008	Submit report to Virginia DOE with revised AUP and Internet Safety program. Full implementation of Internet Safety program

Professional Development

Summer, 2007	Acceptable Use Regulation training for administrative staff
Sept., 2007	Site-based Acceptable Use Regulation training for school staff
Yearly in Sept.	Annual review of AUP by all PWCS staff
Dec., 2007	Professional development for Instructional Technology Resource Teachers
Jan. - Feb., 2008	Face to face and online professional development for schools that will pilot the Internet Safety curriculum
Spring, 2008	Face to face and online professional development for all schools

Community Outreach and Training

- Internet Safety presentation at annual Technology Showcase
- School-based parent and community meetings
- Collaboration with PWC Police Department and School Resource Officers to develop Internet safety protocols and curriculum
- Use of available public communications (PWCS television network) to provide Internet safety information to parents and the community

PURCHASE ORDER

2011

PO Number: PC 041033P11-357
Page #: 1 **PO Date:** 07/12/10
Contract#:
Delivery Date: 07/12/10
Confirmation? No **FOB:** Destination

Ship To Address
Dept. of Information Technology (033A)
Prince William County Public Schools
Edward L. Kelly Leadership Center - Room #1400
14715 Bristow Road
MANASSAS, VA 20112

Prince William County Public Schools

Vendor Address VS
Patriot Technologies, Inc
5108 Pegasus Ct
Suite F
Frederick, MD 21704
DBA Name:

Bill To Address
Dept. of Information Technology
Prince William County Public Schools
P.O. Box 389

MANASSAS, VA 20108

PWCPS Contact: Jim Hite / Jason Dasher
Phone /Email: 703-791-8722 / 703-791-8112

Last Print/Modification Date: 07/12/10
Grand Total Amount: $ $68,461.31

Special Instructions:

Quote provided by Christina Albert on 7/7/10
Any concerns regarding the contract terms and conditions contact the Central Purchasing Office, Daemien Jones, 703-791-8740

Contractor shall deliver all items in accordance with GSA Contract GS-35F-0563U

Westcon

c/o Patriot Technologies
5108 Pegasus Court, Suite F, Frederick, MD 21704

GSA Schedule GS-35F-0563U, Expiration 9/4/2013

Line	Commodity Code/Description	Quantity	Unit	Unit Price	Amount	Qty Rec
1	96200 Services (not already listed) BLUE COAT RENEWAL / FY 2011 / Estimate # Q000000752 Item Part Quantity Unit Price Extended Price 1 HRTFS1R-SG200-A 1.00 EA $37.58 Blue Coat Renewal, Return To Factory, Support, Hardware Only, 1 YR, SG200-A Period Of Performance: 4/1/2010 - 7/1/2011 HW Serial: 1406060024 2 SL131R-SG200-A 1.00 EA $436.81 Blue Coat Renewal, Support, 24x7 L1-L3 Software Only, 1 YR, SG200-A Period Of Performance: 4/1/2010 - 7/1/2011 HW Serial: 1406060024 3 HRTFS1R-DIR-510 1.00 EA $151.93 Blue Coat Renewal, Return To Factory, Support, Hardware Only, 1 YR, DIR-510 Period Of Performance: 5/15/2010 - 7/1/2011 HW Serial: 4707101281 4 SL131R-DIR-510 1.00 EA $1,832.44 Blue Coat Renewal, 24X7 L1-L3 Software Support Only, DIR-510 Non-Cert Supp 1 Year Period Of Performance: 5/15/2010 - 7/1/2011 HW Serial: 4707101281 5 SL131R-SG810-D 1.00 EA $5,098.18 Blue Coat Renewal, Support, 24x7 L1-L3 Software Only, 1 YR, SG810-D Period Of Performance: 5/16/2010 - 7/1/2011				9,191.44	

HW Serial: 3706080406

6 HRTFS1R-SG810-D 1.00 EA $427.67
Blue Coat Renewal, Return To Factory, Support, Hardware Only, 1 YR, SG810-D
Period Of Performance: 5/16/2010 - 7/1/2011
HW Serial: 3706080406

7 SL131R-SG510-B 1.00 EA $1,206.83
Blue Coat Renewal, Support, 24x7 L1-L3 Software Only, 1 YR, SG510-B
Period Of Performance: 5/16/2010 - 7/1/2011
HW Serial: 5006101039

FUND	DEPT	UNIT	APPR	OBJ	ACTV	FUNC	BAL	SUB BAL	AMOUNT
001	033	0330	106	3504	0330				9,191.44

Line	Commodity Code/Description	Quantity	Unit	Unit Price	Amount	Qty Rec
2	96200				8,718.53	

Services (not already listed)
CONTINUATION OF ESTIMATE # Q000000752:

Item Part Quantity Unit Price Extended Price

8 HRTFS1R-SG510-B 1.00 EA $101.63
Blue Coat Renewal, Return To Factory, Support, Hardware Only, 1 YR, SG510-B
Period Of Performance: 5/16/2010 - 7/1/2011
HW Serial: 5006101039

9 SL131R-SG810-B 1.00 EA $3,692.35
Blue Coat Renewal, Support, 24x7 L1-L3 Software Only, 1 YR, SG810-B
Period Of Performance: 5/16/2010 - 7/1/2011
HW Serial: 5106081025

10 HSDSS1R-SG810-B 1.00 EA $923.09
Blue Coat Renewal, Same Day Ship, Support, Hardware Only, 1 YR, SG810-B
Period Of Performance: 5/16/2010 - 7/1/2011
HW Serial: 5106081025

11 SL131R-SG810-B 1.00 EA $3,692.35
Blue Coat Renewal, Support, 24x7 L1-L3 Software Only, 1 YR, SG810-B
Period Of Performance: 5/16/2010 - 7/1/2011
HW Serial: 5106081135

12 HRTFS1R-SG810-B 1.00 EA $309.11
Blue Coat Renewal, Return To Factory, Support, Hardware Only, 1 YR, SG810-B
Period Of Performance: 5/16/2010 - 7/1/2011
HW Serial: 5106081135

FUND	DEPT	UNIT	APPR	OBJ	ACTV	FUNC	BAL	SUB BAL	AMOUNT
001	033	0330	106	3504	0330				8,718.53

Line	Commodity Code/Description	Quantity	Unit	Unit Price	Amount	Qty Rec
3	96200				50,551.34	

Services (not already listed)
CONTINUATION OF ESTIMATE # Q000000752:

Item Part Quantity Unit Price

13 SL131R-SG810-B 1.00 EA $3,692.35
Blue Coat Renewal, Support, 24x7 L1-L3 Software Only, 1 YR, SG810-B
Period Of Performance: 5/16/2010 - 7/1/2011
HW Serial: 5106081142

14 HRTFS1R-SG810-B 1.00 EA $309.11
Blue Coat Renewal, Return To Factory, Support, Hardware Only, 1 YR, SG810-B
Period Of Performance: 5/16/2010 - 7/1/2011
HW Serial: 5106081142

15 SL131R-SG8100-20-PR 1.00 EA $13,950.00
Blue Coat Renewal, Support, 24x7 L1-L3 Software Only, 1 YR, SG8100-20-PR
Period Of Performance: 7/2/2010 - 7/1/2011
HW Serial: 408116092

16 HSDSS1R-SG8100-20-PR 1.00 EA $3,487.50
Same Day Ship HW Only
Period Of Performance: 7/2/2010 - 7/1/2011
HW Serial: 408116092

17 SL131R-SG8100-20-PR 1.00 EA $13,950.00
Blue Coat Renewal, Support, 24x7 L1-L3 Software Only, 1 YR, SG8100-20-PR
Period Of Performance: 7/2/2010 - 7/1/2011
HW Serial: 3707111042

18 HSDSS1R-SG8100-20-PR 1.00 EA $3,487.50
Same Day Ship HW Only
Period Of Performance: 7/2/2010 - 7/1/2011
HW Serial: 3707111042

19 RNW-SVC-BCWF-20K-49K-1Y 1.00 EA $10,925.07
Blue Coat Renewal Service, Blue Coat WebFilter, 20,000-49,999 Users, 1 Yr.
Period Of Performance: 5/16/2010 - 7/1/2011
HW Serial: QA456-KP525
Notes: Quantity = 20000

20 SL131R-RPT-EE 1.00 EA $749.81
Blue Coat Renewal, 24X7 L1-L3 Software Support Only, RPT-EE Non-Cert
Supp 1 Year
Period Of Performance: 5/16/2010 - 7/1/2011
HW Serial: full-unlimitedperp-08E9-347e

Total Order Amount: $68,461.31

FUND	DEPT	UNIT	APPR	OBJ	ACTV	FUNC	BAL SUB BAL	AMOUNT
001	033	0330	106	3504	0330			50,551.34

Line	Commodity Code/Description	Quantity	Unit	Unit Price	Amount	Qty Rec
4	96200 Services (not already listed) CONTINUATION OF ESTIMATE # Q000000752: NOTES: Products are being offered on GSA from Patriot via a participating GSA Dealer program with Westcon. Please use the following information when issuing a Purchase Order: Westcon					

PO Number:
PC 041033P11-357

PURCHASE ORDER

c/o Patriot Technologies
5108 Pegasus Court, Suite F, Frederick, MD 21704
GSA Schedule GS-35F-0563U, Expiration 9/4/2013
TIN: 52-1957100
Cage Code: 07FD4 DUNS: 933945248

Please send purchase orders to:
RFQ@patriot-tech.com or fax to 301-695-4711

Notes: Sale Amount: 68,461.31
Order Disc (0.00%): 0.00
Sales Tax: 0.00
Misc Charges: 0.00
Total Amount: $68,461.31

FUND	DEPT	UNIT	APPR	OBJ	ACTV	FUNC	BAL	SUB	BAL	AMOUNT
001	033	0330	106	3504	0330					

GRAND TOTAL: *$68,461.31*

SCHOOL/DEPT SIGNATURE

8/20/10
DATE

[✓ *Final*]
Partial

This order has been electronically approved. The purchase order number referenced above must be on all invoices, packaging slips and correspondence. Refer to PWCPS website *http://www.pwcs.edu/purchasing* for applicable terms and conditions. **Shaded areas on this printed purchase order are for internal use only.**

PO Number:
PC 041033P10-302

PURCHASE ORDER

2010

Page #
1

PO Number:	PC 041033P10-302
Page #:	1
PO Date:	08/31/09
Contract#:	
Delivery Date:	08/31/09
Confirmation?	No
FOB:	Destination

Providing A World-Class Education

Prince William County Public Schools

Ship To Address
Dept. of Information Technology (033A)
Prince William County Public Schools
Edward L. Kelly Leadership Center - Room #1400
14715 Bristow Road
MANASSAS, VA 20112

Vendor Address VS
Patriot Technologies, Inc
5108 Pegasus Ct
Suite F
Frederick, MD 21704

DBA Name:

Bill To Address
Dept. of Information Technology
Prince William County Public Schools
P.O. Box 389

MANASSAS, VA 20108

PWCPS Contact: Jim Hite / Jason Dasher
Phone /Email: 703-791-8722 / 703-791-8112

Last Print/Modification Date: 08/31/09
Grand Total Amount: $ $85,534.92

Special Instructions:

Westcon Group Noth America, GS-35F0563U c/o
PATRIOT TECHNOLOGIES, INC, GSA Schedule GS-35F-4363D.

Price quoted by Dawn Bradley on 8/13/09
Any concerns regarding the contract terms and conditions contact the Central Purchasing Office, Daemien Jones, 703-791-8740

Line	Commodity Code/Description	Quantity	Unit	Unit Price	Amount	Qty Rec
1	20800 Software see line 4					

FUND	DEPT	UNIT	APPR	OBJ	ACTV	FUNC	BAL	SUB BAL	AMOUNT
001	033	0330	106	3401	0330				

Line	Commodity Code/Description	Quantity	Unit	Unit Price	Amount	Qty Rec
2	96200 Services (not already listed) Invoice # 27349 line 190 (page 3) NO. 190 : BC-PS-CONSULT-ON-SITE BlueCoat Professional Services/Qty: 5 @ $2,000.00 each / ext price $10,000 NOTE: Travel & Expenses are TBD & not included in Prof Svcs NO. 191 : PS -Travel-Reimburse/BlueCoat Travel & Expenses to be billed @ actuals & to be determined based on length of engagement & location. QTY: 1 NOTE: Above professional services are not available via GSA schedule and have been quoted OPEN Market. ALL TRAVEL EXPENSES FOR THIS ORDER ARE NOT TO EXCEED $2,000.00				10,000.00	✓

FUND	DEPT	UNIT	APPR	OBJ	ACTV	FUNC	BAL	SUB BAL	AMOUNT
001	033	0330	106	3401	0330				10,000.00

Line	Commodity Code/Description	Quantity	Unit	Unit Price	Amount	Qty Rec
3	20800 Software see line 5					

PO Number:
PC 041033P10-302

PURCHASE ORDER

FUND	DEPT	UNIT	APPR	OBJ	ACTV	FUNC	BAL	SUB BAL	AMOUNT
001	033	0330	106	3401	0330				

Line	Commodity Code/Description	Quantity	Unit	Unit Price	Amount	Qty Rec
4	20800 Invoice # 27349 Page 1 + 2, Software BLUECOAT RENEWAL: NO. 20 : BC-HRTFS1R-SG200-A BlueCoat Renewal, Return to Factory, Standard Support, Hardware Only/1 YR/SG200-A/ Qty: 1 @ $30.00/ POP: 4/1/09-4/1/10 - SN # 1406060024 NO. 30 : BC-SL131R-SG200A BlueCoat Renewal, Standard Support, 24x7 L1-L3 Software Only/ 1 YR/SG200-A/Qty: 1 @ $348.75 / POP: 4/1/09-4/10/10 - SN#1406060024 NO. 40 : BC-HRTFS1R-DIR-510 BlueCoat Renewal, Return to Factory, Standard Support, Hardware Only/1 YR/DIR-510/Qty:1 @ $134.25/ POP: 5/15/2009 - 5/15/2010 - SN # 4906101149 NO. 50 : BC-SL131R-DIR-510 BlueCoat Renewal, Standard Support, 24x7, L1-L3, Software Only/1YR/DIR-510/Qty:1 @ $1,619.25/POP 5/1/09-5/15/10- SN#4906101149 NO. 60 : BC-SL131R-SG810-D BlueCoat Renewal, Standard Support, 24X7 L1-L3 Software Only/ 1YR/SG810-D/Qty:1 @ $4,519.00/POP:5/16/09-5/16/10-SN # 3706080406 NO. 70 : BC-HRTFS1R-SG810-D BlueCoat Renewal, Return to Factory, Standard Support, Hardware Only/1 YR/SG810-D/Qty:1 @ $378.75/POP: 5/16/09 - 05/16/10 - SN #3706080406 NO. 80 : BC-SL131R-SG510-B BlueCoat renewal, Standard Support, 24X7 L1-L3 Software Only/ 1YR/SG510-B/Qty: 1 @ $1,068.75/POP:5/16/09-5/16/10-SN# 5006101039 NO. 90 : BC-HRTFS1R-SG810-B BlueCoat Renewal, Return to Factory, Standard Support, Hardware Only/1YR/SG810-B/Qty: 1 @ $273.75/POP: 5/16/09-05/16-10 - SN # 5006101039 NO. 100 : BC-SL131R-SG810-B BlueCoat Renewal, Standard Support,24x7, L1-L3 Software Only /SG810-B/Qty: 1 @ $3,270.00/POP: 5/16/09-5/16/10 - SN #5106081025 NO. 110 - BC-HSDSS1R-SG810-B BlueCoat Renewal/Same Day Ship/Standard Support/Hardware Only/1Yr/SG810B/Qty:1@ $817.50/ POP:5/16/09-5/16/10 - SN # 5106081025 NO. 120: BC-SL131R-SG810-B BlueCoat Renewal/Standard Support/24x7 L1-L3 Software only/ 1Yr/SG810B/Qty:1@ 3,270.00/POP: 5/9/09-5/16/10 - SN #5106081135 NO. 130 : BC-HRTFS1R-SG810-B BlueCoat Renewal, Return to Factory/Standard Support/Hardware Only/1YR/SG810-B/Qty:1 @ $273.75/POP:5/16/09-5/16/10 -SN # 5106081135 NO. 131 : BC-SL131R-SG810-B BlueCoat Renewal/Standard Support/24x7 L1-L3/Software Only/1YR/SG810-B/Qty: 1 @ $3,270.00/POP: 5/16/09-5/6/10 - SN # 5106081142 NO. 132 : BC-HRTFS1R-SG810-B BlueCoat Renewal, Return to Factory/Standard Support/Hardware Only/1Yr/SG810-B/Qty: 1 @ $273.75/POP:05/16/09-5/16/10 - SN # 5106081142 NO. 140 : BC-SL131R-RPT-EE BlueCoat Renewal/Standard Support/24x7 L1-L3 Software only/1yr/RPT-EE/Qty: 1 @ 445.50 - SN # full-unlimited-perp-08E9-347e NO. 150 : BC-SL131R-SG8100-20-PR BlueCoat Renewal/Standard Support/24x7 L1-L3 Software only/1Yr/SGB-100-20-PR/Qty:1 @ $13,950.00/POP:7/2/09-7/1/10- SN# 0408116092				54,868.00	

PURCHASE ORDER

NO. 160 : BC-HSDSS1R-SG8100-20-PR BlueCoat Renewal, Same Day Ship/Standard Support/Hardware Only/1Yr/SG8100-20-PR/Qty: 1 @ $ 3,487.50/POP:7/2/09-7/01/10 - SN # 0408116092

NO. 170 : BC-SL131R-SG8100-20-PR BlueCoat Renewal/Standard Support/24x7 L1-L3 Software Only/1Yr/SG8100-20PR/
Qty: 1 @ 13,950.00/POP:7/2/09-7/1/10- SN # 3707111042

NO. 180 : BC-HSDSS1R-SG8100-20-PR BlueCoat renewal, Same Day Ship/Standard Support/hardware Only/1Yr/SG8100-20PR/Qty: 1 @ $3,487.50/POP:7/2/09-7/1/10 - SN # 3707111042

FUND	DEPT	UNIT	APPR	OBJ	ACTV	FUNC	BAL	SUB BAL	AMOUNT
001	033	0330	106	3504	0330				54,868.00

Line	Commodity Code/Description	Quantity	Unit	Unit Price	Amount	Qty Rec
5	20800 Software SSL LICENSE:				20,666.92	

Invoice # 27688 Page 1 of 1

NO. 210 : SW-SSL-SG8100-20 BlueCoat SSL License, SG8100-20Qty:2@$8,261.96 each ext price $16,523.92

NO. 220 : BC-SSL-SG810D - BlueCoat SSL License and Card, SG810-D /Qty:1 @ $4,143.00

FUND	DEPT	UNIT	APPR	OBJ	ACTV	FUNC	BAL	SUB BAL	AMOUNT
001	033	0330	106	3504	0330				20,666.92

GRAND TOTAL: $85,534.92

SCHOOL/DEPT SIGNATURE	2/12/10 DATE	[✓ Final] Partial	This order has been electronically approved. The purchase order number referenced above must be on all invoices, packaging slips and correspondence. Refer to PWCPS website *http://www.pwcs.edu/purchasing* for applicable terms and conditions. **Shaded areas on this printed purchase order are for internal use only.**

' Call ID: 00525010 Status: Open

Customer/School ID	First Name	Last Name	Title
OPHS	Kenneth	Hansen	TSSPEC
Phone, Extension	Direct Phone	e-mail ID	
7033656500 608	(703) 365-6564	GAHAGACJ@pwcs.edu	
Department/School	Address		AssignGroup
Osbourn Park High	8909 Euclid Avenue Manassas 20111		Zone 1

Call Record

		Chronology			**Signed off By**
		Received by			
Tracker	HMC	HMC	10/06/2010	09:20:31am	**CloseGroup**
Call Status	**Open**	Last Update			
		nicholma	01/03/2011	06:47:19am	
Call Type	InfoSec - Content Filter [redacted]	Closed By			
			/ /	: :	
Priority	4 Workstation				

Call Description

TICKET STATUS: INSTRUCTIONAL TECHNOLOGY EVALUATING REQUEST.

CONTENT FILTER REQUEST: UNFILTER <gayrights.change.org > | TICKET <525010>

Cause

Close Description

Assignment

Group	Vendor Call #		Assignment Status		
School		Assigned by	HMC	10/06/2010	09:20:32am
Assignee		[redacted]	hansenkc	10/06/2010	09:22:04am
OPHS		[redacted]	hansenkc	10/06/2010	09:22:05am
Phone, Extension	Pager				
608	7033664733				
e-mail ID					
hansenkc@pwcs.edu					

Assignment

Group	Vendor Call #		Assignment Status		
Help Desk		Assigned by	hansenkc	10/06/2010	09:22:08am

Assignee		[redacted]	avilasb	10/06/2010	09:43:03am
		[redacted]	avilasb	10/06/2010	09:43:04am
Phone, Extension	Pager				
e-mail ID					

Assignment

Group	Vendor Call #		Assignment Status		
Security		Assigned by	avilasb	10/06/2010	09:43:05am
Assignee		[redacted]	hansenkc	01/01/2011	02:13:59pm
		[redacted]	hansenkc	01/01/2011	02:14:00pm
Phone, Extension	Pager				
e-mail ID					

Assignment

Group	Vendor Call #		Assignment Status		
Help Desk		Assigned by	hansenkc	01/01/2011	02:14:04pm
Assignee		[redacted]	nicholma	01/03/2011	06:47:12am
		[redacted]	nicholma	01/03/2011	06:47:12am
Phone, Extension	Pager				
e-mail ID					

Assignment

Group	Vendor Call #		Assignment Status		
Security		Assigned by	nicholma	01/03/2011	06:47:14am
Assignee		[redacted]		/ /	: :
		[redacted]		/ /	: :
Phone, Extension	Pager				
e-mail ID					

Journal Entry

Entered by avilasb 10/06/2010 09:43:10am

Journal Type

Memo

It is blocked by the County

Journal Entry

Entered by briggsdt 12/14/2010 12:09:03pm

Journal Type

Memo

Message:
I have a student working on her research paper and on Monday was able to browse to

gayrights.change.org

and today it is blocked. Please verify the accuracy of this block.

Thank you,
Carrie Gahagan

User Context: GAHAGACJ.Employee.OsbournPark.HS.PWCS
Phone: 703-365-6500
Location: Osbourn Park HS
Workstation ID: OPHS-321872 - 00:18:71:7D:E3:AE Workstation.OsbournPark.HS.PWCS

Journal Entry

Entered by briggsdt 12/14/2010 12:10:24pm

Journal Type

Memo

>>> Briggs, Darryl (Darryl Briggs) 12/14/2010 12:12 PM >>>

TICKET STATUS: INSTRUCTIONAL TECHNOLOGY EVALUATING REQUEST.

CONTENT FILTER REQUEST: UNFILTER <gayrights.change.org > | TICKET <525010>

Please review the following

website/url.

Ticket Notes:
Message:
I have a student working on her research paper and on Monday was able to browse to

~~gayrights.change.org~~

and today it is blocked. Please verify the accuracy of this block.

Thank you,
Carrie Gahagan

User Context: GAHAGACJ.Employee.OsbournPark.HS.PWCS
Phone: 703-365-6500
Location: Osbourn Park HS
Workstation ID: OPHS-321872 - 00:18:71:7D:E3:AE.Workstation.OsbournPark.HS.PWCS

Darryl Briggs

Information Security Specialist
Department of Information Technology
Prince William County Public Schools
briggsdt@pwcs.edu
Phone (703) 791-7493

****
CONFIDENTIALITY NOTICE:
The information transmitted in this email is intended only for the person or entity to which it is addressed and may contain confidential and/or legally privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. Messages can be "forwarded" to another recipient ONLY at the original sender's discretion. If you have received this e-mail in error, please notify the sender immediately either by using the reply facility on your e-mail system or by the number(s) listed above and delete the material from your computer.
****

Journal Entry Entered by hansenkc 01/01/2011 02:11:40pm

Journal Type

Memo

Is this website being reviewed? If it will stay blocked by the county can you then close it with a close discription so the ITRT, Teachers and Librarian could know that it will not get unblocked?

Customer/School ID		First Name	Last Name	Title
BFHS		Carl	Binsted	TSSPEC
Phone, Extension		Direct Phone	e-mail ID	
(571) 261-4400	629	(571) 261-4460	ReevesKD@pwcs.edu	
Department/School		Address		AssignGroup
Battlefield High		15000 Graduation Drive, Haymarket, VA 2016		Zone 1

Call Record

Tracker	helpdesk		
Call Status	**Closed**		
Call Type	InfoSec General		Missinq I...
Priority	4	Workstation	

Chronology

Received by		
helpdesk	04/25/2008	10:34:42am
Last Update		
alvaredm	10/07/2008	12:41:24pm
Closed By		
alvaredm	10/07/2008	12:41:24pm

Signed off By
Security
CloseGroup
Security

Call Description

CONTENT FILTER REQUEST: fca.org TICKET 308841

I am submitting a ticket for a block investigation as I've been instructed to do by DITS. Thanks in advance for looking into this! It's a question of regulation enforcement.

If "dayofsilence.org" is blocked because it's a noncurricular organization (specifically, GLSEN) as we've been told, then shouldn't an organization like FCA (fca.org) also be blocked for the same reason?

If we're going to enforce regulations, don't we have an objective obligation to apply those regulations with equality? I'm interested in what the higher-ups would have to say. If it's just an oversight because no one has suggested it... consider it suggested!

I am NOT an advocate for blocking such sites. I'd rather the school division not foray into this territory at all and literally avoid the issue, but as the organization does block sites on bases

Cause Request

close ticket

other than offensive content, I'm hoping to prompt an examination from a policy perspective to ensure the equal application of the rules. Thanks!

User Context: ReevesKD.Battlefield.HS.PWCS
Phone: 571-261-4400
Location: Battlefield HS
Workstation ID: BFHS-289293 - 00:04:75:94:9B:10.Workstations.Battlefield.HS.PWCS

Assignment

Group	Vendor Call #
School	
Assignee	
BFHS	
Phone, Extension	Pager
629	7033664734
e-mail ID	
binstece@pwcs.edu	

Assignment Status

Assigned by	helpdesk	04/25/2008	10:34:42am
Acknowle...	binstece	04/25/2008	02:43:52pm
Res...	binstece	04/25/2008	02:43:55pm

Assignment

Group	Vendor Call #
Help Desk	
Assignee	
Phone, Extension	Pager
e-mail ID	

Assignment Status

Assigned by	binstece	04/25/2008	02:43:59pm
Acknowle...	avilasb	04/28/2008	07:13:32am
Res...	avilasb	04/28/2008	07:13:33am

Assignment

Group	Vendor Call #
Security	
Assignee	

Assignment Status

Assigned by	avilasb	04/28/2008	07:14:03am
Acknowle...	alvaredm	04/30/2008	09:05:14am

Res... alvaredm 10/07/2008 12:41:22pm

Phone, Extension Pager

e-mail ID

Journal Entry

Entered by binstece 04/25/2008 02:43:22pm

Journal Type

Memo

Moving ticket to helpdesk since I can't do a thing with it.

Journal Entry

Entered by alvaredm 05/14/2008 01:47:21pm

Journal Type

Memo

Submit to Ginny

sent Ginny instructions on how to access unrestricted account and gave her username and password to access.
will follow up on Monday regarding instructions.

Journal Entry

Entered by alvaredm 06/20/2008 11:18:57am

Journal Type

Memo

Hi Ginny, have you seen this ticket? Also, have you been able to access the unrestricted account to view these sites? I wanted to know if we could close this ticket.

Thanks!
Diego

Journal Entry

Entered by alvaredm 06/20/2008 11:22:59am

Journal Type

Memo

Hi Diego - Yes to both questions. I have the unrestricted settings on my laptop, since it is not always open and I can control that access on that computer very well, and it is working well.

I did look at that site - and discussed the issue with Jason. I don't see the curricular integration on that one and can see the FCA integration to the county's Wellness initiative. Jason was going to write something to Keith I think, but I did not follow up to see if that had happened.
Ginny

Blue Coat

Blue Coat WebFilter URL Categories

The Blue Coat WebFilter™ database contains Web site ratings representing billions of Web pages, published in more than 50 languages, and organized into useful categories to enable customers to better monitor, control, and secure their Web traffic. Blue Coat WebFilter is supported by Blue Coat's powerful WebPulse cloud community. WebPulse accurately categorizes up to 98% of unrated objectionable sites in real-time to better enforce customer policy and makes that information immediately available to all customers (see Blue Coat WebFilter data sheet for more details). The following is an alphabetical listing and description of the categories currently used by Blue Coat WebFilter to classify Web sites.

CATEGORIES[1]

Abortion

Sites that provide information or arguments in favor of or against abortion, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion.

Adult/Mature Content

Sites that contain material of adult nature that do not necessarily contain excessive violence, sexual content, or nudity. These sites include very profane or vulgar content and sites that are not appropriate for children.

Alcohol

Sites that offer for sale, promote, glorify, review or in any way advocate the use or creation of alcoholic beverages, including but not limited to beer, wine, and hard liquors. This does not include sites that sell alcohol as a subset of other products such as restaurants or grocery stores.

Alternative Sexuality/Lifestyles

Sites that provide information, promote, or cater to alternative sexual expressions in their myriad forms. Includes but is not limited to the full range of non-traditional sexual practices, interests, orientations or fetishes. This category does not include sites that are sexually gratuitous in nature which would typically fall under the Pornography category, nor does it include lesbian, gay, bisexual, transgender or any sites that speak to one's sexual identity.

Alternative Spirituality/Belief

Sites that promote and provide information on alternative spiritual and non-religious beliefs such as atheism, agnosticism, witchcraft, and Satanism. Occult practices, voodoo rituals or any other form of mysticism are represented here. This includes sites that endorse or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, incantations, curses and magic powers. The category includes sites that discuss or deal with paranormal or unexplained events.

Art/Culture

Sites that nurture and promote cultural understanding of fine art including but not limited to sculpture, paintings and other visual art forms, literature, music, dance, ballet, and performance art and the venues or foundations that support, foster or house them such as museums, galleries, symphonies and the like. Sites that provide a learning environment or cultural awareness outside of the strictures of formalized education such as planetariums are included under this heading.

Auctions

Sites that support the offering and purchasing of goods between individuals. This does not include classified advertisements.

Audio/Video Clips

Sites that provide streams or downloads of audio or video clips – typically 15 minutes or less in length. This also includes sites that provide downloaders and players for audio and video clips.

Blogs/Personal Pages

Sites that primarily offer access to personal pages and blogs. This classification includes but is not limited to content that shares a common domain such as Web space made available by an ISP or some other hosting service. Personal home pages and blogs tend to be dynamic in nature and their content may vary from innocuous to extreme.

Brokerage/Trading

Sites that provide or advertise trading of securities and management of investment assets (online or offline). This also includes insurance sites as well as sites that offer financial investment strategies, quotes, and news.

Business/Economy

Sites devoted to business firms, business information, economics, marketing, business management and entrepreneurship. This does not include sites that perform services defined in another category (such as information technology companies, or companies that sell travel services). This does not include shopping sites.

Charitable Organizations

Sites that foster volunteerism for charitable causes. This also encompasses non-profit associations that cultivate philanthropic or relief efforts. Does not include organizations that attempt to influence legislation as a significant portion of their activities or organizations that campaign for, contribute to, or affiliate with political organizations or candidates.

Chat/Instant Messaging

Sites that provide chat, text messaging (SMS) or instant messaging capabilities or client downloads.

Computers/Internet

Sites that sponsor or provide information on computers, technology, the Internet and technology-related organizations and companies.

Content Servers

Servers that provide commercial hosting for a variety of content such as images and media files. These servers are typically used in conjunction with other Web servers to optimize content retrieval speeds.

Education

Sites that offer educational information, distance learning, or trade school information or programs. This also includes sites that are sponsored by schools, educational facilities, faculty, or alumni groups.

Email

Sites offering web-based email services, such as online email reading and mailing list services.

[1] Categories and their definitions as of July 28, 2009

Entertainment

Sites that provide information on or promote mass entertainment media including but not limited to film, film trailers, television, home entertainment, music, comics, entertainment-oriented periodicals, reviews, interviews, fan clubs, and celebrity gossip. This also includes wedding or other photography sites of a non-adult nature.

Extreme

Sites that are extreme in nature and are not suitable for general consumption. This includes sites that revel and glorify in gore, human or animal suffering, scatological or other aberrant behaviors, perversities or debaucheries. It includes visual or written depictions deemed to be of an unusually horrific nature. These are salacious sites bereft of historical context, educational value or artistic merit created solely to debase, dehumanize or shock. Examples would include necrophilia, cannibalism, scat and amputee fetish sites.

Financial Services

Sites that provide or advertise banking services (online or offline) or other types of financial information, such as loans. This does not include sites that offer market information, brokerage or trading services.

For Kids

Sites designed specifically for children. This category is typically used in conjunction with other categories – it is not a stand-alone category.

Gambling

Sites where a user can place a bet or participate in a betting pool, participate in a lottery, or receive information, assistance, recommendations, or training in such activities. This category does not include sites that sell gambling-related products/machines or sites for offline casinos and hotels, unless they meet one of the above requirements.

Games

Sites that support playing or downloading video games, computer games, or electronic games. This includes sites with information, tips, or advice on such games or how to obtain cheat codes, and also includes magazines dedicated to computerized games and sites that support or host online sweepstakes and giveaways.

Government/Legal

Sites sponsored by or that provide information on government, government agencies and government services such as taxation and emergency services. This includes sites that discuss or explain laws of various governmental entities. This also includes sites that advertise legal services, lawyers for hire, adoption services, information about adoption, immigration information, and immigration services.

Greeting Cards

Sites that facilitate the sending of electronic greeting cards, animated cards, or similar electronic messages typically used to mark an event or occasion.

Hacking

Sites that distribute, promote, or provide hacking tools and/or information which may help gain unauthorized access to computer systems and/or computerized communication systems. Hacking encompasses instructions on illegal or questionable tactics, such as creating viruses, distributing cracked or pirated software, or distributing other protected intellectual property.

Health

Sites that provide advice and information on general health such as fitness and well-being, personal health or medical services, drugs, alternative and complementary therapies, medical information about ailments, dentistry, optometry, general psychiatry, self-help, and support organizations dedicated to a disease or condition.

Humor/Jokes

Sites that primarily focus on comedy, jokes, fun, etc. This may include sites containing jokes of adult or mature nature. Sites containing humorous Adult/Mature content also have an Adult/Mature category rating.

Illegal Drugs

Sites that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.

Illegal/Questionable

Sites that advocate or give advice on performing acts that are illegal or of questionable legality such as service theft, evading law enforcement, fraud, burglary techniques, and plagiarism. This also includes sites that promote scams or that provide or sell legally questionable educational materials such as term papers.

Internet Telephony

Sites that facilitate Internet telephony or provide Internet telephony services such as voice over IP (VOIP).

Intimate Apparel/Swimsuit

Sites that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. This does not include sites selling undergarments as a subsection of other products offered.

Job Search/Careers

Sites that provide assistance in finding employment and tools for locating prospective employers.

LGBT

Sites that provide information regarding, support, promote, or cater to one's sexual orientation or gender identity including but not limited to lesbian, gay, bisexual, and transgender sites. This category does not include sites considered sexually gratuitous in nature that would typically fall under the Pornography category.

Media Sharing

Sites that allow sharing of media (e.g., photo sharing) and have a low risk of including objectionable content such as adult or pornographic material.

Military

Sites that promote or provide information on military branches or armed services.

Network Errors

Requests for uncategorized sites that cannot be completed due to some temporary or permanent network error condition including requests for invalid or non-existent URLs. Because these requests do not result in the retrieval of Web content, this category is not returned directly from Blue Coat WebFilter. Rather, it is reported via Blue Coat Reporter to help administrators more accurately account for uncategorized requests that do not result in the retrieval of Web content.

News/Media

Sites that primarily report information or comments on current events or contemporary issues of the day. This category also includes news radio stations and news magazines but does not include sites that can be rated in other categories.

Newsgroups/Forums

Sites that primarily offer access to newsgroups, messaging or bulletin board systems, or group blogs where participants can post comments, hold discussions, or seek opinions or expertise on a variety of topics.

Non-viewable

Servers with non-malicious, non-offensive content or resources used by applications, but not directly viewable by web browsers. Includes but is not limited to Web analytics sites (such as visitor tracking and ranking sites) and content filtering systems.

Nudity

Sites containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect but may include sites containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist sites that contain pictures of nude individuals.

Online Meetings

Sites that facilitate online meetings or provide online meeting, conferencing, or training services.

Online Storage

Sites that provide secure, encrypted, off-site backup and restoration of personal data. These online repositories are typically used to store, organize and share videos, music, movies, photos, documents, and other electronically formatted information. Sites that fit this criteria essentially act as your personal hard drive on the Internet.

Open/Mixed Content

Sites with generally non-offensive content but that also have potentially objectionable content such as adult or pornographic material that is not organized so that it can be classified separately. Sites that explicitly exclude offensive content are not included in this category.

Pay to Surf

Sites that pay users in the form of cash or prizes for clicking on or reading specific links, email, or Web pages.

Peer-to-Peer (P2P)

Sites that distribute software to facilitate the direct exchange of files between users. P2P includes software that enables file search and sharing across a network without dependence on a central server.

Personals/Dating

Sites that promote interpersonal relationships.

Phishing

Sites that are designed to appear as a legitimate bank or retailer with the intent to fraudulently capture sensitive data (e.g., credit card numbers, PIN numbers).

Placeholders

Sites that are under construction, parked domains, search-bait or otherwise generally have no useful value.

Political/Activist Groups

Sites sponsored by or that provide information on political parties, special interest groups, or any organization that promotes change or reform in public policy, public opinion, social practice, or economic activities.

Pornography

Sites that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.

Potentially Unwanted Software

Sites that distribute software that is not malicious but may be unwanted within an organization such as intrusive adware and hoaxes.

Proxy Avoidance

Sites that provide information on how to bypass proxy server features or gain access to URLs in any way that bypasses the proxy server. This category includes any service which will allow a person to bypass the Blue Coat filtering system, such as anonymous surfing services.

Radio/Audio Streams

Sites that provide streams or downloads of radio, music, or other audio content – typically more than 15 minutes in length.

Real Estate

Sites that provide information on renting, buying, or selling real estate or properties. This also includes vacation property rentals such as time-shares and vacation condos.

Reference

Sites containing personal, professional, or educational reference, including online dictionaries, maps, censuses, almanacs, library catalogues, genealogy-related sites and scientific information.

Religion

Sites that promote and provide information on conventional or unconventional religious or quasireligious subjects, as well as churches, synagogues, or other houses of worship. This does not include sites about alternative forms of spirituality or ideology such as witchcraft or atheist beliefs (Alternative Spirituality/Belief).

Remote Access Tools

Sites that primarily focus on providing information about and/or methods that enable authorized remote access to and use of a desktop computer or private network.

Restaurants/Dining/Food

Sites that list, review, discuss, advertise, and promote food, catering, dining services, cooking, and recipes.

Search Engines/Portals

Sites that support searching the Internet, indices, and directories.

Sex Education

Sites that provide information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, tips for better sex, and sexual enhancement products.

Shopping

Sites that provide or advertise the means to obtain goods or services with either prices listed or a clear way to order. This does not include sites that can be classified in other categories (such as vehicles or weapons).

Social Networking

Sites that enable people to connect with others to form an online community. Typically members describe themselves in personal Web page profiles and form interactive networks, linking them with other members based on common interests or acquaintances. Instant messaging, file sharing and Web logs (blogs) are common features of Social Networking sites. Note: These sites may contain offensive material in the community-created content. Sites in this category are also referred to as "virtual communities" or "online communities". This category does not include more narrowly-focused sites, like those that specifically match descriptions for Personals/Dating sites or Business sites.

Society/Daily Living

Sites that provide information on matters of daily life. This includes but is not

limited to pet care, home improvement, fashion/beauty tips, hobbies, and other tasks that comprise everyday life. It does not include sites relating to entertainment, sports, jobs, personal pages, or other topics that already have a specific category.

Software Downloads

Sites that are dedicated to the electronic download of software for any type of computer or mobile device, whether for payment or at no charge.

Sports/Recreation

Sites that promote or provide information about spectator sports or recreational activities. This does not include sites dedicated to hobbies such as gardening, collecting, board games, scrapbooking, quilting, etc.

Spyware Effects/Privacy Concerns

Sites to which spyware (as defined in the Spyware/Malware Sources category) reports its findings or from which it alone downloads advertisements. This does not contain sites that serve advertisements for other Web pages in addition to spyware advertisements; only those sites uniquely used by spyware. Includes sites that contain serious privacy issues, such as "phone home" sites to which software can connect and send user information; and sites to which browser hijackers redirect users. This usually does not include sites that can be categorized as Spyware/Malware Sources.

Spyware/Malware Sources

Sites that host or distribute spyware and other malware or whose purpose for existence is as part of the spyware and malware ecosystem. Spyware and malware are defined as software that takes control of a computer, modifies computer settings, or collects or reports personal information without the permission of the end user. This includes software that misrepresents itself by tricking users to download or install it, or to enter personal information. This includes sites that perform drive-by downloads; browser hijackers; dialers; any program that modifies your browser homepage, bookmarks, or security settings; and keyloggers. This also includes any software that bundles spyware (as defined above) as part of its offering. Information collected or reported is "personal" if it contains uniquely identifying data, such as email addresses, name, social security number, IP address, etc. A site is not classified as spyware if the user is reasonably notified that the software will perform these actions (e.g., it alerts that it will send personal information, be installed, or that it will log keystrokes).

Suspicious

Sites considered to have suspicious content and/or intent that poses an elevated security or privacy risk. This categorization is determined by analysis of Web reputation factors. This also includes sites that are part of the Web and email spam ecosystem. If a site is determined to be clearly malicious or benign, it will be placed in a different category.

Tobacco

Sites that offer for sale, promote, glorify, review or in any way advocate the use or creation of tobacco or tobacco related products including but not limited to cigarettes, pipes, cigars and chewing tobacco. This does not include sites that sell tobacco as a subset of other products such as grocery stores.

Translation

Sites that allow translation of text (words, phrases, Web pages, etc.) between various languages or that can be used to identify a language.

Travel

Sites that promote or provide opportunity for travel planning, including finding and making travel reservations, sharing of travel experiences (pro or con), vehicle rentals, descriptions of travel destinations, or promotions for hotels/casinos or other travel related accommodations. Mass transit information including but not limited to posting of schedules, fares or any other public transportation-related data are also included in this category.

TV/Video Streams

Sites that provide streams or downloads of television, movie, or other video content – typically more than 15 minutes in length.

Uncategorized

These show in the ProxySG logs as the category 'none'.

User-Defined

Requests given a custom classification by an ProxySG administrator.

Vehicles

Sites that provide information on or promote vehicles, boats, or aircraft, including sites that support online purchase of vehicles or parts.

Violence/Hate/Racism

Sites that depict extreme physical harm to people, animals, or property, or that advocate or provide instructions on how to cause such harm. This also includes sites that advocate or depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics, and includes content that glorifies self-mutilation or suicide.

Weapons

Sites that sell, review, or describe weapons such as guns, knives, or martial arts devices, or provide information on their use, accessories, or other modifications. This does not include sites providing information on BB guns, paintball guns, black powder rifles, target shooting, or bows and arrows, unless the site also meets one of the above requirements. Also does not include sites that promote collecting weapons, or groups that either support or oppose weapons use.

Web Advertisements

Sites that provide online advertisements or banners. This does not include advertising servers that serve adult-oriented advertisements.

Web Applications

Sites with interactive, Web-based office/business applications. This excludes email, chat/IM or other sites that have a specific content category.

Web Hosting

Sites of organizations that provide top-level domain pages, as well as Web communities or hosting services.

Blue Coat Systems, Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA USA // +1.408.220.2200

EMEA Headquarters
Hampshire, UK // +44.1252.554600

APAC Headquarters
Hong Kong // +852.3476.1000