FOIA request regarding filtering software
Avoca School District 37
Wilmette, IL

Background
In the summer of 2010, the district switched its filtering system from SonicWall to LightSpeed. Since the SonicWall was decommissioned in 2010, we have no ability to provide any logs from that period. The LightSpeed logging is set up to maintain logs for only 40 days (the default is 7 days for the items the district is interested in logging).

1. The LightSpeed category that identifies LGBT "Gay or Lesbian or Bisexual Interest" is called "Education.lifestyles". This category is being blocked for the student policy and for the default policy. It is allowed for the teacher policy.

2. The district's use of Internet Filtering software to block the following web sites:

a. Day of Silence http://dayofsilence.org is categorized under the Education.lifestyles category and is blocked

b. It Gets Better Project http://itgetsbetter.org is categorized under the Photography category and is NOT blocked

c. The Trevor Project http://thetrevorproject.org is categorized under the Family.health category and is NOT blocked

d. The GSA Network http://gsanetwork.org is categorized under the Educational.lifestyles and is blocked

e. Gay, Lesbian, Straight Education Network http://glsen.org is categorized under the Educational.lifestyles and is blocked

3. All requests to block or unblock any site first go to the Avoca onsite team for approval. No such requests were made regarding this topic

4. See attached spreadsheet of "Default Policy".

5. No decisions were made to block or unblock the sites in questions. Avoca deferred to the default settings regarding these topics and have not altered them.

6. The category that identifies LGBT is Educational.lifestyles. This remains blocked by default in the district for students, but open for adults.

7. None

8. Just the normal subscription renewals for the Internet Filtering solution.

9. See attached Acceptable Use Policy

AVOCA SCHOOL DISTRICT #37
2921 Illinois Road, Wilmette, IL 60091
(847) 251-3587

TECHNOLOGY ACCEPTABLE USE POLICY

Authorization for Technology Access
Each staff member and student's parent/guardian must sign this Authorization as a condition for using District technology connections. School Board members and administrators are treated like staff members for purposes of this Authorization. Please read this document carefully before signing.

Rights and Responsibilities
All use of technology shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This *Acceptable Use Policy* does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow the terms of the *Acceptable Use Policy* may result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The signature(s) at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

Usage Guidelines

1. Acceptable Use – Access to District technology must be for the purpose of education or research, and be consistent with the educational objectives of the District.

2. Privileges – The use of District technology is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges and/or discipline up and to expulsion in the case of students or suspension or dismissal in the case of staff. The Superintendent or designee with consult from necessary parties will make all decisions regarding whether or not a user has violated this *Policy* and may deny, revoke, or suspend access at any time.

3. Unacceptable Use – The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

    a. Knowingly using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State regulation;
    b. Unauthorized downloading of software, regardless of whether it is copyrighted or devirused;
    c. Downloading copyrighted material for other than personal use;
    d. Using the network for private financial or commercial gain;
    e. Wastefully using resources, such as file space;
    f. Hacking or gaining unauthorized access to files, resources, or entities;
    g. Intentionally invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature.
    h. Using another user's account or password;
    i. Posting material authored or created by another without his/her consent;
    j. Posting anonymous messages;
    k. Using the network for commercial or private advertising;
    l. Intentionally accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material;
    m. Using the network while access privileges are suspended or revoked; and,
    n. Using encrypted communication without prior approval from the Superintendent or designee.
    o. Using the network for fundraising.

4. Software Use

    a. Avoca School District #37 licenses the use of copies of computer software from a variety of publishers and distributors. The District does not own the copyright to this software or its related documentation and, unless authorized by the software publisher, does not have the right to reproduce it for use on more than one computer.
    b. Avoca School District #37 is committed to providing all users with information about intellectual property and copyright law and the policies for requisition, utilization, and auditing.
    c. With regard to use on local area networks (LANs) or on multiple machines, Avoca School District #37 users will use the software only in accordance with the license agreement.
    d. Avoca School District #37 will explain the internal control procedures for metering the use of software, maintaining purchase orders and license agreements, penalties for illegal use, and budget and acquisition procedures.
    e. Avoca School District #37 users who learn of any misuse of software or related documentation within the District will notify the Superintendent or designee.
    f. According to U.S. copyright law, illegal reproduction of software is subject to civil damages of as much as U.S. $100,000 per title infringed, and criminal penalties, including fines of as much as U.S. $250,000 per title infringed, and imprisonment of up to five years. District users who make, acquire, or use unauthorized copies of software will receive due process as appropriate under the circumstance. Such due process may include termination. Avoca School District #37 does not condone the illegal duplication of software and will not tolerate it.

5. Hardware – All computer hardware and peripherals used in the District for either administrative or instructional use must be purchased through the Avoca Business Office. Equipment purchased with District funds outside of the Avoca Business Office will not be supported, will not be asset tagged, and will not be insured.

6. Network Etiquette – You 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 become abusive in your messages to others.
    b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
    c. Do not reveal the personal information, including the addresses or telephone numbers of students or colleagues.
    d. Recognize that electronic mail (E-mail) is not private. People who operate the system 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 any way that would disrupt its use by other users.

7. No Warranties – The Board makes no warranties of any kind, whether expressed or implied, for the service it is providing. The Board will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The Board denies any responsibility for any information, including its accuracy or quality, obtained or transmitted through use of the Internet. Further, the Board denies responsibility for any information that may be lost, damaged, altered, or unavailable when using the Internet.

8. Indemnification – The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this *Policy,* including such incurred through copyright violation.

9. Security – Network security is a high priority. If you can identify a security problem on the network, you must notify the Superintendent or designee. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. 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 may be denied access to the network.

10. Use of Electronic Mail

    a. The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.
    b. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
    c. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail that would be inappropriate in a letter or memorandum.
    d. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this School District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
    e. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the Superintendent or designee. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
    f. Use of the School District's electronic mail system constitutes consent to these regulations.

11. Internet Safety

    a. Internet access is limited to only those "acceptable uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in these procedures, and otherwise follow these procedures.
    b. Staff members shall supervise and monitor students while students are using District Internet access.
    c. Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or designee. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:
        - Limiting student access to inappropriate matter as well as restricting access to harmful materials;
        - Student safety and security when using electronic communications;
        - Limiting unauthorized access, including "hacking" and other unlawful activities; and
        - Limiting unauthorized disclosure, use, and dissemination of personal identification information.
    d. The Superintendent, designee, and staff shall monitor student Internet access.

12. Vandalism – Vandalism will result in cancellation of privileges and other disciplinary action up and to expulsion in the case of students or suspension or dismissal in the case of staff. Vandalism is defined as any malicious attempt to harm or destroy technology or data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

13. Charges – The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs. Any and all such unauthorized charges or fees shall be the responsibility of the user.

14. Confidentiality – Employees shall maintain confidentiality of student records in their use of District computers. Confidential student information should not be loaded onto the network without prior administrative approval.

15. Monitoring of Personal Use – As a condition of using the Internet, including electronic mail communication, through District computers or Internet access, employees consent to monitoring and inspection by school administration of personal use of District computers. Such monitoring and inspection shall include any and all electronic mail communications made or attempted to be made or received by users and all materials downloaded by users.

16. Copyright Web Publishing Rules – Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District Web sites or file servers without explicit written permission.

    a. For each republication (on a Web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.
    b. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying the material may not be considered a source of permission. Permission must be in written (not electronic or verbal) form.

ADDENDUM TO AVOCA SCHOOL DISTRICT 37
TECHNOLOGY ACCEPTABLE USE POLICY
Remote Access to District Network

District 37 will enable middle school students and District teachers to access most features of its technology system from home and from other remote locations, using laptop computers provided and owned by the District. This step is being taken in keeping with the District's Technology Plan, so that members of its learning community can take full advantage of the educational resources available through use of school technology connections. E-mail and instant messaging capability will not be accessible on the District system from remote locations.

When using this privilege of remote access to the technology system, including filtered access to the Internet via that system, every user is expected to comply with the District's technology Acceptable Use Policy without regard to his or her location. Violations of the Policy by users who access the system from remote locations may result in loss of system privileges, school disciplinary measures, and appropriate legal action to the same extent as if the violations had occurred at school.

The District will monitor school use and conduct periodic checks of District-provided laptop computers and hard drives in order to detect and prevent violations of the Acceptable Use Policy. However, parents of students who are afforded the privilege of remote access should be aware that District 37 cannot supervise online activities of students who are using the technology system from remote locations. The District encourages parents to monitor and help promote their students' beneficial use of this valuable learning tool.

Category Name	Cat #	Description	Default
Local-Allow	1	Local Override of Blocked Domains	Allowed
Local-Block	2	Local Override of Allowed Domains	Blocked
ads	3	Ad servers and advertising companies	Allowed
adult	4	Adult Products, Services, Situations of humor	Blocked
audio-video	5	Sources of MP3s, mpegs, and streaming	Allowed
business	6	Business	Allowed
errors	7	Content database errors waiting to be purged	Allowed
drugs	8	Sites promoting illicit and illegal drug use	Blocked
education	9	Education and reference sites	Allowed
business.finance	10	Banking, stock markets, insurance, and financial news	Allowed
forums	11	Unmoderated Personal Expression	Blocked
gambling	12	Gambling, casinos, betting, lottery and play-for-cash/sweepstakes	Blocked
games	13	Games, anime, cartoons, wallpapers and screen savers	Allowed
general	14	General interest	Allowed
government	15	Federal, state, local and international government	Allowed
security.hacking	16	Computer hacking	Blocked
violence.hate	17	Sites that promote hate against different groups	Blocked
business.jobs	18	Employment search, offerings and support	Allowed
forums.mail	19	Email sites	Blocked
news	20	News, Magazines, TV News Stations and Radio News stations	Allowed
porn	21	Pornography related sites	Blocked
porn.de	22	German pornography sites	Blocked
porn.es	23	Spanish pornography sites	Blocked
porn.fr	24	French pornography sites	Blocked
porn.it	25	Italian pornography sites	Blocked
porn.jp	26	Japanese pornography sites	Blocked
porn.nl	27	Dutch pornography sites	Blocked
security.proxy	28	Web proxy servers and open SMTP relays	Blocked
shopping	29	Shopping sites	Allowed
sports	30	Sports sites	Allowed
suspicious	31	Recently discovered sites with suspicious words or phrases	Blocked
violence	32	Sites promoting violence and anarchy	Blocked
security.warez	33	Sites promoting illegal access and sharing of software and other copyrighted material	Blocked
directory	34	Directories and portals about specialized topics	Allowed
ads.popup-ads	35	Popup ads	Allowed
travel	36	Hotels, resorts, cruises, transportation and vacation offerings	Allowed
automobile	37	Automobiles and motorcycles	Allowed
forums.newsgroups	38	Newsgroups, usenet and subscription newsletters	Blocked

forums.personals	39	Personal web pages and personal ads	Blocked
humor	40	Humor, puzzles, and brain-teasers	Allowed
education.lifestyles	41	Education about lifestyles - gay, lesbian, alternate	Allowed
alcohol	42	Production, promotion and sale of alcoholic beverages	Blocked
family.health	43	Health care	Allowed
education.science	44	Science and technology	Allowed
entertainment	45	Movies, television, radio, and celebrities	Allowed
kids_and_teens	46	Kid safe web sites	Allowed
education.arts	47	Art, art history, architecture, graphic design,and illustration	Allowed
education.literature	48	Literature, libraries, writers	Allowed
music	49	Bands and artists, concerts, DJs, lyrics, songwriting, and record labels	Allowed
education.music	50	Music education, history, instruments, marching, and museums	Allowed
microsoft	51	Microsoft and related sites	Allowed
ads.banner-ads	52	Banners ads	Allowed
ads.html-ads	53	HTML ads	Allowed
ads.javascript-ads	54	Javascript ads	Allowed
spam	55	Sources of spam mail that does not involve porn, gambling, or drugs	Allowed
ham	56	Legitimate sources of email	Allowed
computers	57	Computers & Internet	Allowed
family.religion	58	Religion & Spirituality	Allowed
world	59	Sites about regions and languages of the world	Allowed
forums.p2p	60	Peer to peer sites	Blocked
forums.im	61	Instant messaging	Blocked
security.spyware	62	Spyware - advertising supported software	Blocked
security.virus	63	Viruses, malware, trojans, backdoors, hacker tools	Blocked
security.test	64	Used for testing virus signatures and registry controls	Allowed
security.phishing	65	Web sites of internet scams that try to get personal information	Blocked
violence.weapons	66	Web sites about guns, swords, knives, and other weapons	Blocked
access-denied	67	Sites of Pages that Deny Access, or are unauthorized to access	Blocked
law	68	Law firms, courts, and legal matters	Allowed
kids_and_teens.chat	69	Monitored chat websites suitable for kids	Allowed
adult.language	70	Strong language	Blocked
forums.blogs	71	Webblogs	Blocked
security	72	Security risks	Blocked
business.real_estate	73	Real estate, homes, offices	Allowed
education.games	74	Educational games for kids	Allowed
education.social_sciences	75	Social sciences	Allowed
family.food	76	Restaurants, grocery stores, recipes	Allowed
kids_and_teens.animals	77	Cats, dogs, horses and other animals	Allowed

shopping.spam	78	Shopping websites that use spam email for marketing	Allowed
society	79	Culture, issues, ethnicity, people	Allowed
education.sex	80	High school level sex education websites	Allowed
shopping.auctions	81	Auctions	Allowed
sports.fantasy	82	Fantasy football, baseball, soccer, etc.	Allowed
hobby	83	Hobbies, crafts, collecting	Allowed
sports.youth	84	High schools sports teams and youth sports leagues	Allowed
search	85	Major search engines	Allowed
world.de	86	World websites - German	Allowed
world.es	87	World websites - Spanish	Allowed
world.fr	88	World websites - French	Allowed
world.it	89	World websites - Italian	Allowed
world.jp	90	World websites - Japanese	Allowed
world.nl	91	World websites - Netherlands	Allowed
world.pt	92	World websites - Portuguese	Allowed
world.ru	93	World websites - Russian	Allowed
porn.child	94	Porn sites involving children	Blocked
family	95	Family life, cooking,gardening, home improvement	Allowed
society.politics	96	Politics, political activism, political issues	Allowed
society.crime	97	Crime and the justice system	Allowed
sports.martial_arts	98	Martial arts	Allowed
education.history	99	History	Allowed
adult.art	100	Adult art	Blocked
adult.bodyart	101	Body art, tattoos, body piercings	Blocked
adult.games	102	Adult games	Blocked
adult.lifestyles	103	Adult lifestyles	Blocked
shopping.office_supplies	104	Major office supply websites	Allowed
expired	105	Domains whose registration has expired	Allowed
world.pl	106	World websites - Polish	Allowed
world.cn	107	World websites - Chinese	Allowed
world.kr	108	World websites - Korean	Allowed
porn.pl	109	Polish pornogrphy sites	Blocked
porn.ru	110	Russian pornography sites	Blocked
porn.pt	111	Portuguese pornography sites	Blocked
plagiarism	112	Websites that sell term papers, research papers and other ways to help students cheat	Allowed
parked	113	Web sites using internet scams in an attempt to get personal information	Blocked
suspicious.script	114	Websites whose only content is javascript - frequently used to hiding porn sites	Blocked
business.construction	115	Construction, building, plumbing, home improvement	Allowed
security.nettools	116	Net tools, remote admin tools, internet server and client applications	Allowed

forums.social_networking	117	Social networking and related websites such as myspace.com, facebook.com, orkut.com	Blocked
forums.dating	118	Dating websites such as friendfinder.com, eharmony.com, match.com, etc.	Blocked
business.manufacturing	119	Manufacturing, industrial, and shipping companies	Allowed
G-Rated	120	G-Rated	Allowed
PG-Rated	121	PG-Rated	Allowed
R-Rated	122	R-Rated	Blocked
X-Rated	123	X-Rated	Blocked
S-Rated	124	S-Rated	Blocked
security.potentially_unwant	125	Potentially unwanted applications	Blocked
offensive	126	Websites considered to be offensive to both adults and children	Blocked
computers.filehosting	127	Image, filehosting, shareware, freeware websites	Blocked
computers.consumer_electr	128	Consumer electronics - TVs, cell phones, MP3 players, etc.	Allowed
education.media	129	Educational streaming media resources	Allowed
security.virus_ignore	130	Virus signatures that should be ignored	Blocked
entertainment.radio_and_tv	131	Radio and TV stations	Allowed
photography	132	Photography	Allowed