BEST PRACTICES

Filtering Internet content in a library environment creates certain obligations. It's a more demanding process than parents face when filtering their children's computers or for employers filtering their workers PCs. Neither parents nor employers need to bother about protecting their children's privacy or ensuring their employees have free access to information.

In 1948, the American Library Association adopted the Library Bill of Rights, which "affirms that all libraries are forums for information and ideas, and that the following basic policies should guide their services.

I. Books and other library resources should be provided for the interest, information, and enlightenment of all people of the community the library serves. Materials should not be excluded because of the origin, background, or views of those contributing to their creation.

II. Libraries should provide materials and information presenting all points of view on current and historical issues. Materials should not be proscribed or removed because of partisan or doctrinal disapproval.

III. Libraries should challenge censorship in the fulfillment of their responsibility to provide information and enlightenment.

IV. Libraries should cooperate with all persons and groups concerned with resisting abridgment of free expression and free access to ideas.

V. A person's right to use a library should not be denied or abridged because of origin, age, background, or views.

VI. Libraries which make exhibit spaces and meeting rooms available to the public they serve should make such facilities available on an equitable basis, regardless of the beliefs or affiliations of individuals or groups requesting their use."[30]

The library is incumbent to make a concerted effort to implement technology protection measures in accordance with the above policies and to promote the library as an institution committed to building an informed, literate citizenry whose right to privacy, speech, and expression are safe-guarded.

This chapter discusses best practices for implementing an Internet filter in a public library setting. These guidelines are intended to assist libraries using filters for some or all of their library computers, to comply with CIPA, or to satisfy the community's demand for additional safeguards for children. Although filtering policies will vary, the goal of every library choosing to filter should be to implement the technology according to the long-held beliefs and traditions associated with providing public library service.

Protect patron privacy—do not use monitor feature

Filter profiles define the action that will be taken for each category of content for a particular user or group of users.

The actions that can be chosen may include block, warn, monitor, or allow. In a library, few categories should be chosen for any action besides 'allow' for adult patrons and staff. Each library's filtering strategy determines the degree to which other categories will be chosen to block, warn, or monitor for the patron profile.

Because protecting patron privacy is critical, libraries should not use the monitor feature. In rare situations, monitoring has been used to isolate illegal use of library computers.

Generally, librarians have no reason to monitor, in real-time, anyone's Internet use. Summary reports of websites accessed by patrons, with no link to a specific patron, provide enough information to monitor the effectiveness of the filter without the need to violate a person's privacy.

Learn the filter company's categories

Most filters hide the specific URLs that have been placed in each category. Libraries cannot be sure what sites will be denied when the category is selected for blocking. Reading the category name, however, does not necessarily give the administrator a clear idea of what type of content is contained in the category. Reading the descriptions of the category is crucial.

Filter companies concoct their own schemes for categorizing websites. No authority exists to rely on for interpretation based on the category headings. The best the administrator can do is study the descriptions for each category and monitor the sites that are blocked as a result of selecting that category.

To demonstrate the nonstandard nature of category headings, consider the library that wishes to block pornography for its young adult patrons but doesn't want to block sites containing information about sexual development, sexuality, or sex education.

In the case of Smartfilter, the administrator would choose to block the sex category to accomplish this goal. In contrast, choosing the sex category from N2H2's filter categories would result in blocking more content than was intended.

Smartfilter "Sex"[28]

This category contains URLs that reference, discuss, or show pornography, including pictures, videos, or text of sex acts, or sexually oriented material. This content includes soft- and hard-core pornography, sado-masochism, bestiality, and so on. Some examples are:

- PORN USA
- Hustler

Note: In the broader context of cultural norms and individual taste, it may be debatable what is considered sex or pornography or simply a form of entertainment. In a standard business or educational setting, though, URLs contained in this category are considered unproductive.

N2H2 "Sex"[29]

Sites that contain descriptions or depictions of sexual acts, specifically those without the intent to arouse (sites that contain material intended to arouse fall under the pornography category). Sexual merchandise and fetish sites fall under the sex category.

Examples:

www.handbooktogreatsex.com

http://members.aol.com/Sebringsil

www.joaniblank.com/sexuality.htm

Each filter uses a unique system for naming categories, and the filters sometimes use words in unexpected ways. The filter administrator must become familiar with the filter categories to learn what the filter company really means by its headings.

Do not rely on any kind of shared definition of the words in the content category heading. Consider one filter's definition of its sexuality category as compared with the definition from the *American Heritage Dictionary*.

American Heritage Dictionary of the English Language

Sexuality 1. The condition of being characterized and distinguished by sex. 2. Concern with or interest in sexual activity. 3. Sexual character or potency.

iPrism

Sexuality This category contains those sites that provide information, images or implications of bondage, sadism, masochism, fetish, beating, body piercing, or self-mutilation.

Even reading the headings and descriptions of the content category and examining the sample sites that are sometimes provided doesn't tell the administrator exactly what websites are included in any given category, but it does provide an important start.

Use filter to reinforce policies associated with activities

Filters can be used to limit activities as well as access to content. If your library has policies about how different computers are used, the filter profiles can often be designed to reinforce those policies.

Using the example of a filter with six content categories (adult, pornography, gambling, hate, games, weapons), the filter profiles might look like this:

Sample library filter profiles (Extensively blocking content)

Staff	**Adult**	**Youth**	**Children**
Adult—allow	Adult—allow	Adult—block	Adult—block
Pornography—block	Pornography—block	Pornography—block	Pornography—block
Gambling—allow	Gambling—allow	Gambling—allow	Gambling—block
Hate—allow	Hate—allow	Hate—warn	Hate—block
Games—allow	Games—allow	Games—allow (block 3 p.m. to 6 p.m.)	Games—block
Weapons—allow	Weapons—allow	Weapons—allow	Weapons—block

Filter profiles can be used to comply with CIPA, but they also can be used to reinforce other aspects of the Internet use policy. For example, in the previous sample library filter policy, games are allowed under the Youth profile except between the hours of 3 p.m. and 6 p.m. This policy may be because the library is attempting to restrict the use of the young adult computers to homework or because other problems have been encountered that are associated with too many children monopolizing computers after school.

Filters might be able to help enforce policies that have previously not been enforceable without staff intervention. Identify and account for these non-CIPA issues before a filter is selected to ensure the filter can address as many of these policies as possible.

Use multiple profiles to accommodate different filtering levels

Using multiple profiles, the library can customize filtering for staff, adults, young adults, grade schoolers, and young children. Involve staff from each library department in devising filter profiles for the patrons they serve. After all, the departmental staffer will have to respond to overblock complaints and requests to completely disable the filter.

Profiles can usually be associated with a login or a computer (IP address). The result is that a person logging into a computer as 'youth' or simply selecting one of the youth terminals will have certain categories of content set to 'block' as defined by the library.

For example, using a product such as N2H2's Bess[30], you might choose to block the following categories for each of the library's three types of patrons:

Adults	**Youth**	**Children**
Pornography	Adults only	Auction
	Gambling	Chat
	Illegal	Drugs
	Pornography	Electronic commerce
		Gambling
		Games
		Message/bulletin boards
		Nudity
		Personal information
		Personals
		Pornography
		Sex
		Violence

Defining filtering profiles for specific groups of patrons is the best way to comply with CIPA while addressing the expectation of many parents that the library is a safe place for their children to learn.

The previous list may be more broad than is suitable for one library but less comprehensive than another library requires. Select a filter that allows the library the flexibility needed to implement filtering as instructed by the board or in a way that responds to the community's needs.

Minimally block to comply with CIPA

For legal definitions related to CIPA see llrx.com/features/updatecipa.htm.

Obscene material and depictions of child pornography are already illegal, and libraries have no reason to allow this type of content to any patron or staff. Theoretically, any library blocking only this type of content would never have to worry about unblocking blocked sites or turning off filters.

No filter, however, actually limits its categories to obscene material and child pornography because the current definition of obscenity doesn't work on the Internet. Two prongs of the three-part Miller test[31] that establishes whether something is obscene relies on community standards. When viewing content over the Internet, saying what constitutes the community is difficult. Such a finding is practically impossible to make for Internet content.

Also, the Miller test states that the content as a whole must appeal to the prurient interests. But what constitutes the whole when talking about Internet content? Is it the Web page, the website, the domain? Filter companies are less capable of defining obscene Internet content than the local library staff person is because at least the staff person can establish the community he or she is servicing. For these reasons, no filter exists that truly only blocks content mandated by CIPA.

Most filters have a pornography category or some other category for sexually explicit material but no specific child pornography or obscene category. Although filters may claim to be CIPA compliant, they have no CIPA category.

The category of sexually explicit or pornography categories may contain obscene material or child pornography, but they also probably contain soft-core porn sites and nudity.

Commercial products tend to define some type of broad pornography category, which will be the one category libraries will choose if the library's goal is to minimally block content while using an off-the-shelf product.

For example, using CyberPatrol, a well-known filter often used in schools or by parents has no suitable category for blocking access to only illegal sexually explicit content such as obscenity and child pornography. The best you could do is select its adult/sexually explicit category described as follows:

CyberPatrol's categories are described at www.surfcontrol.com/products/content/internet_databases/url_category_list/default.aspx.

Adult/sexually explicit

- Adult products including sex toys, CD-ROMs, and videos
- Adult services including videoconferencing, escort services, and strip clubs
- Erotic stories and textual descriptions of sexual acts
- Explicit cartoons and animation
- Online groups, including newsgroups and forums, that are sexually explicit in nature
- Sexually oriented or erotic full or partial nudity
- Depictions or images of sexual acts, including animals or inanimate objects used in a sexual manner
- Sexually exploitive or sexually violent text or graphics
- Bondage, fetishes, genital piercing
- Nudist sites that feature nudity
- Erotic or fetish photography, which depicts nudity

Although the adult/sexually explicit category might be a suitable category to block for the children's department, it is certainly not suitable for adult patrons. The category goes well beyond the confines of CIPA.

Using a product such as CyberPatrol for complying with CIPA puts you in the position of significantly overblocking content for adult patrons. One way around this problem is to install the filter on adult computers but not select any categories for blocking.

Would a filter configured with no categories selected for blocking (for adult use) comply with CIPA? It might if you had some sites listed in the 'always block' list. Using a product such as CyberPatrol, which is designed for home and school use, requires you to make the decision to not choose any categories for blocking adults or to dramatically overblock adults (as far as CIPA compliance is concerned). Overblocking adults results in more overrides for your staff. The library is better off creatively using the 'always block' and 'never block' lists instead of the overly restrictive categories.

Using a product designed for business use might enable the library to select categories closer to the CIPA-required content. For example, using Websense, the library could set up one filtering profile restricting access to only its sex category:

> "Sex—Sites that depict or graphically describe sexual acts or activity, including exhibitionism; also sites offering direct links to such sites."

Websense's categories are described at http://websense.com/products/about/database/categories.cfm.

In the case of Websense, it distinguishes the previous content from other types of adult material that could still be permitted, such as:

- Adult content—Sites that display full or partial nudity in a sexual context, but not sexual activity; erotica; sexual paraphernalia; sex-oriented businesses as clubs, nightclubs, escort services; and sites supporting online purchase of such goods and services
- Lingerie and swimsuit—Sites that offer images of models in suggestive but not lewd costume, with seminudity permitted. Includes classic cheesecake, calendar, and pinup art and photography. Includes sites offering lingerie or swimwear for sale
- Nudity—Sites that offer depictions of nude or seminude human forms, singly or in groups, not overtly sexual in intent or effect

Search www.lii.org for "children's websites directories" and "children's websites search engines" for more information.

Keep in mind the expectations of parents who believe that libraries using a filter automatically results in a safe experience for their unattended children. Using directories such as KidsClick! and search engines such as Kid's Tools for Searching the Net can help younger children find age-appropriate content on the Internet. Don't rely on the filter to do all the work of helping children browse the Internet safely. Think of the filter as one small part of your toolkit, not the total solution.

Test the configuration before rollout

Filtering software is designed to affect every computer on the library's network, so anything that goes wrong could have a pervasive and negative effect on all library systems. Depending on the filter and how the library has decided to set it up, installation and deployment may require much time in testing and planning before the rollout even begins.

Begin small. Minimally block and test the effects of the filter profiles on a small segment of the network. Use your small test environment to identify changes that need to be made to the profiles and categories. Develop new procedures to handle overblocks, to disable filters, and to respond to complaints about blocked pages.

Identify the ramifications of the filter server or appliance going down. Does a filter shutdown prevent anyone from accessing the Internet or is filtering simply disabled? Test all electronic systems with the test filter in place to ensure the filter doesn't interfere with any services.

Make sure all library Web-based resources can still be accessed with filtering enabled. Don't make the mistake that one librarian made when she installed her filter. She had installed a free filter that she felt was working well except for one problem. The filter was blocking access to the library's Gaylord databases.

This story reinforces the disturbing nature of filter categories. This librarian didn't register that the Gaylord site was blocked because it had the word *gay* in the name so either she had keyword blocking enabled and the word *gay* was one of the forbidden words or anything that looked gay-related was falling into that product's adult category. Her intent was not to block gay-themed content.

This situation amounted to a significant overblock since many key library resources were available through the Gaylord subscription service. Check absolutely everything patrons access via the library home page and intranet to make sure the filter isn't preventing access to anything desired. Don't let patrons identify these problems. This testing is part of the library's cost in setting up and installing the filter.

Expect to pay technical staff and technical consultants to help with installation, testing, and rollout. And account for the staff time associated with this testing phase—that time may be significant.

Publish the library's filtering policy

Share the Internet use policy and the corresponding filtering strategy with the community. Let people know which categories of content have been chosen for blocking for each group of users and why. Give the public an opportunity to discuss the filtering policy and discuss the library and community needs.

Give the public an opportunity to discuss the filtering policy and the library and community needs.

Filtering information can be part of the Internet use policy or can be posted throughout the library near public-access computers. Make finding the information easy for patrons so they can know how and why the library is filtering.

The demand for library use of filters has put the library in the unenviable position of not being able to completely satisfy anyone. Discussing the issues with the community and airing the issues is a good way to receive useful feedback and improve relations with those people opposed to filtering as well as those demanding it.

Monitor the filter's accuracy

Continually monitor the filter's accuracy. The more categories the library has selected for blocking, the bigger the job of monitoring for accuracy becomes because of the increased incidence of overblocking that will naturally occur.

Most filters provide many predefined reports that the administrator can run to help the library track how well the URLs match the content categories, how often patrons encounter blocked pages, which pages have been overridden, the most visited sites, websites using the most bandwidth, and more.

At the least, the library should review the list of sites being blocked by the filter, paying special attention to those sites where an override has been requested. Someone on staff should have the job of reviewing blocked sites and verifying the sites have been categorized properly. The degree to which the library can tolerate overblocks dictates what percentage of sites to review.

Increase the rate of blocked sites reviewed for accuracy by 2% for each blocked category.

For example, a library that only blocks one category of content to minimally comply with CIPA might be satisfied by spot-checking 1% to 2% of the sites blocked each day. Depending on the number of PCs being filtered and whether the actual URLs are made available in the reporting tools or log files, this job could be large or small. Regardless of the job size, perform this minimal level of monitoring.

The more content categories being blocked, the more corrections to overblocking there need to be. According to the Kaiser Family Foundation study[33], the overblocking rate for filters studied was around 2% when the filters were minimally configured to block CIPA content.

This rate, however, increased to as much as 35% with some filters when the goal expanded to restrict access to educational sites only. In other words, the more filters are relied on to control access, the more mistakes there are. Checking only 2% of the blocks when as many as 35% of the blocks are in error will not make much of a dent in the poor accuracy of the library's filter.

A rule of thumb is to increase the percentage of blocked sites reviewed for accuracy by 2% for each category of content selected for blocking.

Solicit patron feedback

One of the best ways to learn about the effectiveness of a filter is to allow for anonymous feedback from patrons. This feedback provides a nonconfrontational way for patrons to advise library personnel when the filtering profiles aren't working for them or they are experiencing inappropriately blocked sites. This feedback opportunity is in addition to the procedures that should be in place to request a site be unblocked or the filter turned off on-the-fly.

The block page sometimes can be used to solicit feedback from patrons. Some filters have a button on the block page that patrons can use to request that a blocked site be reviewed. This feature provides another opportunity for patrons to let their opinions be considered. If such a filter is not offered by the filter itself, the library could provide it as part of its customization of the block page.

Another way to involve patrons is to invite them to assist library staff in reviewing sites that have been blocked, sites that have been requested be unblocked, and to assist in the development of the 'always block' and 'always allow' lists.

Filter Feedback Form

___I'm generally happy with how filtering works in the library but_____

____

____

___I'm generally unhappy with how filtering works because ___________

____

____

___I'd like to suggest the following URL be added to the 'block' list

____

___I'd like to suggest the following URL be added to the 'allow' list

____

[Optional] Name and phone number or e-mail

____

Participating in these evaluations empowers the patrons and gives them a better understanding of how difficult and time-consuming the job of responsibly filtering can be.

Delegate filter-related responsibilities

Systems staff should handle the network and server level responsibilities of the filter, but certain administrative tasks can be delegated to professional and floor staff. For example, staff working directly with patrons should have the ability to override blocked pages. Ideally, any staff person should be able to type a password at the patron workstation to override a block.

Any staff person should be able to type a password at the patron workstation or on any computer in the library to override a block.

Disabling the filter for a given patron might be a job that also can be performed by any person on the floor, depending on how the library's filter requires this action to be done. In some cases, this action only requires the staff person to know the override password or to know the proper unfiltered profile to log the patron into.

In other cases, the filter will require that a change be made at the server console or on the Web-based administrative interface. Accessing the filter's administrative interface requires a special login and password. In this case, only the filter administrator should disable the filter for a user to reduce the number of people with the filter administrator password.

Delegating specific filter administration duties to certain staff in the library can result in quicker service to the patrons, however, it should be done safely. Filters that are designed for delegating some control, such as iPrism and N2H2's filters, generally allow the top-level administrator to define a login and password for other subadministrators and assign them rights in certain areas of the filter's management program.

If the filter doesn't allow for the delegation of administrative tasks, don't delegate duties too broadly. But ensure you have more than one person on staff who can administer the filter, such as an assistant filter administrator.

A larger group of library staff should make decisions associated with filter profiles and content categories. Don't leave these decisions with the filter administrator or assistant administrator. This group should carefully add sites to the 'always allow' or 'always block' lists. Adding a site to the 'always allow' list overrides the category level control that determines when the site will be blocked within each filter profile.

Similarly, library management or a filter monitoring committee, not just systems staff, should evaluate creating a new content category or moving a Web page from one category to another.

Use a filter monitor committee

Just as selecting the filter and developing the Internet use policy is done by a combination of technology, management, and floor staff, so should the ongoing monitoring and evaluation of the filter.

Although technology staff should be responsible for generating reports about sites being blocked, overrides being requested, and the impact of the filter on the library's network, these reports should be reviewed by management and professional staff because they indicate whether the filter is meeting the needs of the library. Asking patrons to participate on this committee is a good way to keep them involved in the decision making, too.

Use staff and community partners to evaluate sites that may have been erroneously blocked.

To ensure that the filtering strategy, as guided by the Internet use policy, is being implemented, a filter monitor committee should meet regularly to review the reports and filter feedback forms submitted by patrons to consider changes for improving the filter's performance. This meeting is especially important in the first months after the filter has been introduced.

Expect to make many adjustments to the filter profiles, filter settings, and procedures, especially in the beginning. Even though the need to adjust the filter will subside over time, monitoring should continue throughout the life of the filter to ensure the library agrees with category decisions made by the filter company.

The dynamic nature of the Internet means that the library will continue to rely on the filter's ability to classify websites, and the library needs to monitor this process.

Train staff and patrons

Training takes many forms. The staff administering the filter need training to ensure they are equipped to handle all the exigencies that may arise with the filter. Appropriate staff should be trained to override erroneously blocked pages or to disable the filter on request. And patrons need to be educated to use the new filtered environment.

Do not introduce filtering to the library without the patron's knowledge. Post signs stating the library's filtering policy—whether the library is filtering or not. If the library is only filtering certain PCs, clearly mark the filtered PCs and the unfiltered PCs.

If all library PCs are filtered and different filtering profiles are used, the library should provide information about the options available for adults and their children. Some parents may prefer their children's Internet access be filtered with an adult profile, but others will want their children's access filtered as strictly as possible.

The ultimate goal of any filtering policy should be to support the diverse needs of the local community. Finding the right balance of filtering is difficult, but the community has the right to know what the library is filtering.

Some members of the community will take the position that the library is censoring constitutionally protected material that they have a right to access. And they are correct.

For this reason, libraries should restrict content as minimally as possible to meet the library's and community's goals. To the extent that patrons understand and appreciate what the library is trying to do and are made to understand that filters are imperfect tools and that adults have the ability to bypass the filter as needed, the library is more likely to earn and keep the community's respect.

Provide key information on the block page

Filters function in many ways but the end result is essentially the same. Content that would normally display on a user's computer screen does not. The users aren't necessarily aware of the filter working behind the scenes until they attempt to view the blocked page, at which point, patrons will most often see a message telling them that access is denied.

Besides policy statements and signs posted around the library, the block page is one of the few ways to directly communicate information about the filtering policy to users of the library computers. This communication should include as much useful information as possible.

Ideally, the default page will include the URL of the blocked site, the categories it encountered that caused the block, any recourse the patron has to override or otherwise challenge the block, and a way to find more pertinent information.

The block page can be designed to include a link to the library's IUP and instructions for how to override the blocked page. Let patrons know that no personally identifying information is retained concerning their Internet use or request to unblock pages. Assure them their privacy is protected.

The URL and category that caused the block must be displayed on the block page, otherwise the patron cannot be sure whether the page was blocked in error. If the page the patron is trying to access is mistakenly blocked and it is the specific page desired, the blocked page or access denied message needs to include everything the patron needs to know to correct the error quickly and easily. (See "Ability To Customize Default Block Page" in Chapter 3.)

Because the Supreme Court opinions made clear that the ability to unblock erroneously blocked sites or to turn off filtering on request is critical to the constitutionality of filtering, make sure the process is easy for both patrons and staff.

Allow patrons to submit anonymous requests to override

Patrons don't always want to ask for help or disclose what they are looking for. The embarrassed teenager looking for sex education information that has been erroneously categorized as sexually explicit and thus blocked is not likely to request the page be unblocked. If patrons could make override requests anonymously, they might.

Some filters allow the user to send an anonymous message requesting the current page be unblocked. Depending on how this unblocking is implemented, it may be automatic or require human intervention.

If the unblock request goes to a person such as the filter administrator, the administrator could first review the requested page to ensure it was erroneously blocked and then allow access. The advantage of having the administrator immediately view the blocked page is to see if it was a mistake that needs to be permanently corrected.

Once evaluated, the administrator can not only permit access to the page but also place the URL in the more appropriate category (or place it on the 'always allow' list, if that is the best option available). Immediately correcting the overblock is better than waiting until the end of the week when blocks are regularly checked for accuracy.

Depending on the page content, the library IUP may dictate that access be permitted only if the patron's age can be verified, in which case anonymous requests to override don't work unless the administrator can verify that the request came from an adult-only terminal or a user using the adult filtering profile.

Another way to use anonymous requests to unblock is to establish a policy that all such requests be honored and then evaluated after the fact. Products that work automatically, rather than requiring the filter administrator to unblock the page, must be used this way.

For the library more concerned about overblocking than underblocking, automatically granting anonymous override requests is the best approach. Under such a scenario, evaluating blocked sites for accuracy after the fact is critical.

Overridden sites often should not have been blocked in the first place, so pay special attention to them. If the site was correctly blocked, ensure the automatic override is not allowed for that page the next time it is requested. This override may be done by placing the site in the 'always block' list or one that doesn't permit automatic overrides.

Even if the filter doesn't allow for anonymous requests to be sent, allow patrons to anonymously submit requests to have sites reevaluated. This ability can be accomplished using a filter feedback form mentioned previously in this chapter.

Use password override to set duration and extent of override

Many products provide a password override option on the block page or system tray on the patron's monitor. The password override can be used by staff to immediately unblock a page at the patron workstation. The best password override features allow an authorized staff person to specify the extent to which filtering will be disabled and for how long.

Password override features can be used to accommodate all disabling requests mandated by the Supreme Court if they are flexible enough. Suppose the library's public access workstations have a 30-minute limit. Setting the password override to 'disable filtering' for up to 30 minutes effectively accommodates the adult user who wishes to browse the Internet unfiltered. Since, per CIPA, this request must be granted by an authorized representative of the library, using the password override is a good way to accomplish this goal. (Also see "Password Override" in Chapter 3.)

Reduce patron requests to unblock or disable filter

The best way to reduce the staff time dedicated to unblocking erroneously blocked sites and disabling and re-enabling filters is to carefully circumscribe the limits of what is being blocked. The better the filter has been configured and fine-tuned, the fewer times patrons will request unblocks.

Numerous requests to work unfiltered should serve as a message that the library is blocking more content than is appropriate for the community's needs. In this case, consider modifying the filter profiles for some public-access terminals so patrons who wish to have less Internet content blocked turn off the filter.

Take advantage of the flexibility inherent in many of the filters that offer many filtering levels for different types of users in your library. This customization will save staff time and keep patrons happier.

Keep filter up-to-date

Every piece of software and hardware requires maintenance in the form of software updates, hardware repairs, and configuration changes. In addition, some filters require daily updates to be downloaded to the content database.

Make one person responsible for the filter's ongoing maintenance. This job is technical and should be performed by the systems staff, just as the technology staff ensures that the virus scanner is always up-to-date and functioning throughout the system.

Ensure Internet access is not interrupted when the filter goes down

Because filters either evaluate or intercept all Internet packets as they flow through the network, have a backup plan for when the filter goes down. For times when the filter is inactive due to server maintenance, configuration error, or hardware failure, make sure the network is configured to bypass the filter server or appliance until the filter comes back online.

Technology staff should work with the vendor to ensure that servers and routers are configured to bypass the filter when needed. Test this eventuality before the filter is rolled out.

Although filtering may be important, Internet access is more important. When the filter is down, libraries should permit unfiltered Internet access.

Notes

[27] American Library Association Bill of Rights. www.ala.org/Content/NavigationMenu/Our_Association/Offices/Intellectual_Freedom3/Statements_and_Policies/Intellectual_Freedom2/Library_Bill_of_Rights.htm.

[28] www.securecomputing.com/index.cfm?skey=86#sx.

[29] http://n2h2.com/products/bess.php?device=categories#sex.

[30] Bess's categories are described at www.n2h2.com/products/categories.php.

[31] Minow, Mary. "Children's Internet Protection Act (CIPA): Legal Definitions of Child Pornography, Obsenity and 'Harmful to Minors.'" LLRX.com (August 31, 2003) www.llrx.com/features/updatecipa.htm.

[32] Hansen, Derek. "CIPA: Which Filtering Software To Use?" Web Junction, August 31, 2003. http://webjunction.org/do/DisplayContent?id=2102.