

THE DAWNING OF THE DIGITAL COMMUNITY

Internet Use Policies and OpenDNS filtering

Jared Leadbetter
Maine State Library

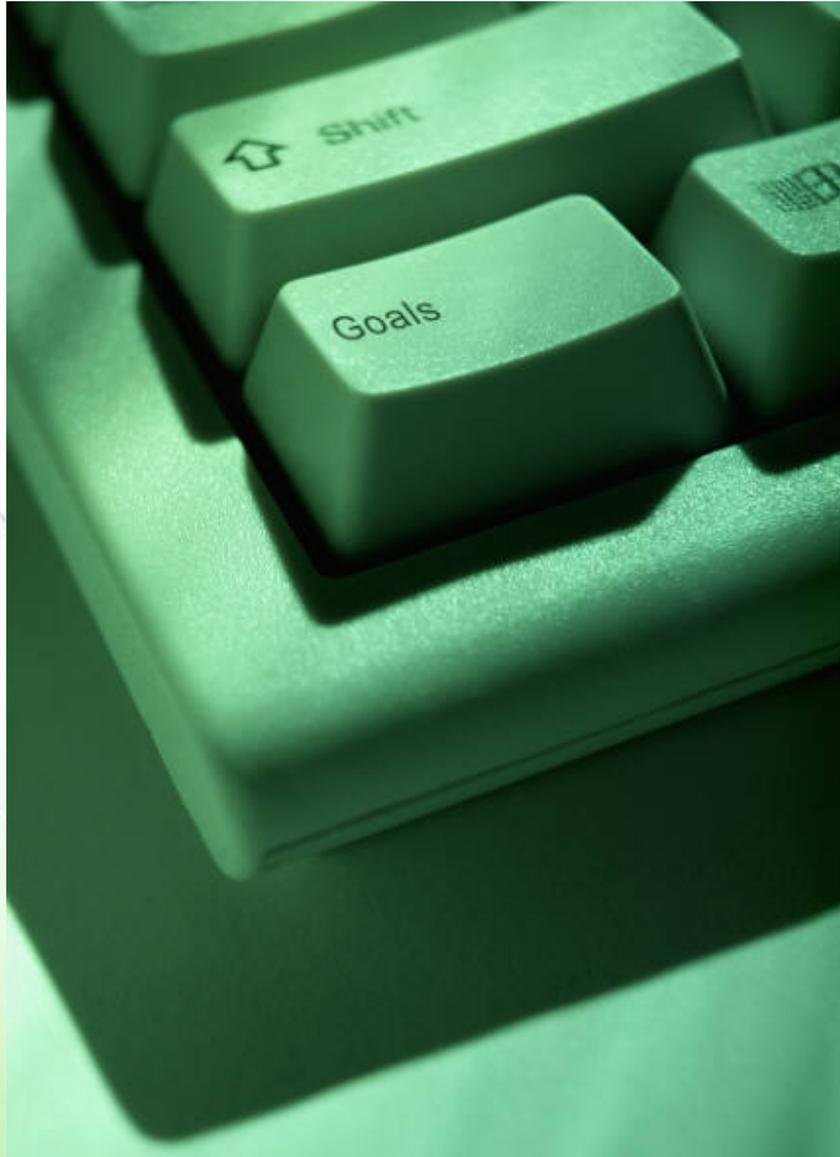


A library is:

- A primary source of access to technology and the Internet for many in the community they serve
- An expert source for information that isn't easily looked up in the phone book or on a search engine
- Serving a diverse population, including young children, teens, adults and seniors, all with different needs and degrees of familiarity with technology
- Expected to balance the ideals of free access to information with the requirements of government and the mores of the community



To do all that, let's:



- Educate ourselves in the living nature of the Internet and the issues surrounding it
- Craft policies that define the library role as information-providers and custodians
- Implement technology measures to protect both the user and the library
- Mentor our users in efficient and responsible use of technology and the Internet

WAKING UP IN THE DIGITAL WORLD



Ten years ago...

Facebook, YouTube and Twitter didn't exist.
In fact...

There were less than fifty million in existence, less than a tenth of the number that exist today. Maybe because...

Penetration of Internet access was significantly less than it is today (about 50% of U.S. households in 2002, 80% in 2012) and dial-up was the predominant connection service (in the U.S.), so...

The Internet back then was just a tiny seed compared to what it has become in 2012.



But also...

The idea of online piracy came into mainstream focus in 2000. It is now said to make up billions of dollars in “lost sales” in the movie and music industries.



Online crime in the U.S. has risen approximately 2000% since 2000; fraud and identity theft take up over 50% of such cases.

Approximately half of the online population of minors have experienced some form of harassment or denigration.

Another 2000% increase occurred in the number of FBI cases of sex crimes against children as a result of online contact between 1996 and 2007.

The Internet is a game-changer for libraries and librarians!

Online
reference

Information ?i →

Social
networking



The picturesque
librarian

E-mail

Business

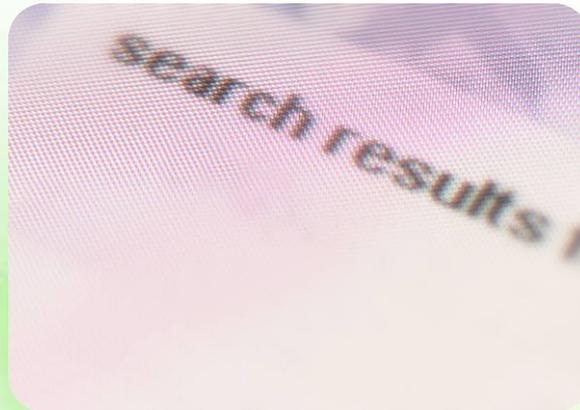
These days...

Librarians are increasingly being asked or expected to teach skills related to the use of technology, especially the Internet and everything on it:



Services – including some that are transitioning to only being online

Searching – helping find good information and instructing the user on self-sufficiency



Security – especially as it pertains to personal information and children



A NEW DAY OF DIGITAL GUIDELINES



Internet Use and Safety Policy

● Mission statement

- Library ethics
- Disclaimers
- Compliance

● Internet safety

- CIPA provisions
- Security
- Etiquette

● Acceptable use

- Session information
- Do and do-nots
- Bypassing filters

● Follow-up

- Whitelisting
- Amending policy
- Public hearing

Mission statement

- Lead with a brief statement as to your library's mission with regard to providing your Internet services.
- Disclaimers regarding to the Internet as an unregulated medium, potentially offensive or harmful to users
- Liability of users (or parents of minors) and statement of not serving *in loco parentis* (in place of the parent)
- Statement of CIPA (Children's Internet Protection Act) filtering (or not filtering) and the imperfection of filtering solutions



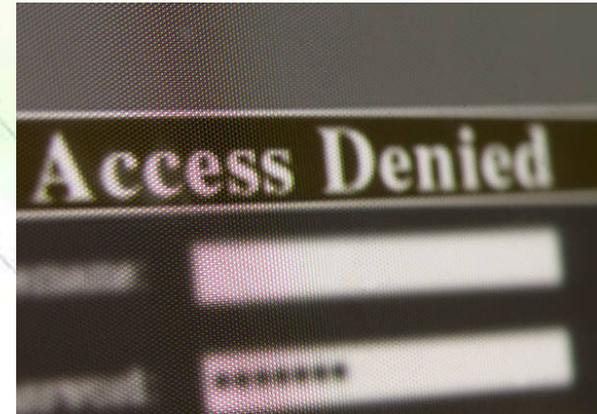
Acceptable use policy

- Description of available services, devices and software
- Using the library technology resources (sign-in, limits on time, age segregation, printing costs, saving files)
- Reference existing library use policies (adding any specific changes with respect to computer use, location or other users)
- Requirements or conditions of use (staff support of hardware or software, user-owned computers and mobile devices)



Unacceptable use

- Legal use issues (harassment, defamation or threats, copyright or license infringement, fraud or identity theft, child pornography)
- Ethical use issues (security or privacy violation, spreading malware or spam, installing unauthorized software, the rights of others)
- Communal use issues (damaging equipment, excessive or improper use of resources, exposing other users to questionable material)
- Consequences (removal of privileges, liability for damages, civil or criminal prosecution)



Internet safety policy

- CIPA provisions (five specific points, bypassing filters, public hearing)
- Safety (personal security, parental involvement, becoming savvy knowledge consumers)
- Etiquette (online interactions, anonymity, cyberbullying, encountering harmful material)
- Education (resources available to users for raising awareness)



CIPA provisions

Five specific points:

- Access by minors to inappropriate matter on the Internet and World Wide Web
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication (including instant messaging)
- Unauthorized access, including “hacking,” and other unlawful activities by minors online
- Unauthorized disclosure, use, and dissemination of personal identification information regarding minors
- Measures designed to restrict minors’ access to material harmful to minors

Bypassing the filter (for bona fide research or other lawful purpose)

Public hearing with reasonable notice (such as an agenda item in a public library board meeting)

Harmful to minors

Any picture, image, graphic image file, or other visual depiction that:

- Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- Depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual conduct, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
- Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors

Follow-up

- **Legal definition or citation (copyright and fair use, American Library Association doctrine, CIPA provisions, obscenity or harmful to minors definition)**
- **Statement of public postings (location of posted documents, web address of page on library policy)**
- **Challenges or appeals (especially with regard to filtering or adding to the whitelist)**
- **Amending or revision policy (dates of changes made to the policy)**



Image by Trey Ratcliffe / www.stuckincustoms.com

 Except where otherwise noted, this work is licensed under <http://creativecommons.org/licenses/by-nc/3.0/>

THE FILTERING LIGHT

What is a filter?

- **A technology protection measure (TPM) that “guards” one or more gateways on the path between the user and available content, and employs some method of selection for permitting or denying access to that content by the user**
- **Where: client-side (on the computer), browsers, search engines, servers and network appliances, ISPs, Internet backbone**
- **How: blacklists or whitelists, keyword recognition, traffic and protocol regulation, removing search results**

Why filter?

(the argument for filtering)

- Compliance with federal regulations means access to federal funds
- Protect our children, even when we're not around
- Are very good at allowing the safe stuff through
- Can be refined to be better with human intervention
- Appeal to some segment of the community served

Why not filter?

(the argument against filtering)

- Maintains the ethics of free speech and access to information without censoring
- Opportunities for learning responsible use are lessened
- They over-block, under-block and can be circumvented
- Require time, money and expertise to set up and maintain
- Can be a source of frustration to some users and legal problems for the library

... and now,

OpenDNS

The existing solution for libraries on MSLN, supported by Networkmaine!

It doesn't just filter, but it acts as another layer of protection from malicious sites and software!

It's free and takes only a few minutes to configure!

Some terms to know:

URL: Uniform Resource Locator. Usually called a “web address,” the chain of words, letters, numbers and other symbols that help people find places on the Internet.

Domain: the pieces of a URL. Domains exist in levels; examples of top-level domains are .com, .org, .gov, .edu, .us, and second-level domains like google.com, nasa.gov or wikipedia.org

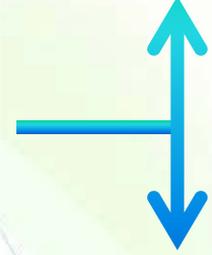
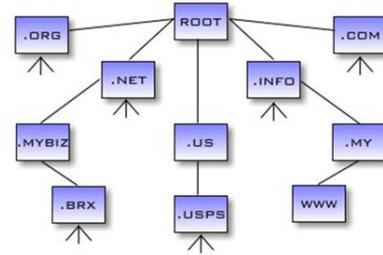
IP (Internet Protocol) Address: the “phone number” by which computers or network are identified

DNS: Domain Name System. The Internet “phone book” used for translating URLs (easy for people) into IP addresses (easy for machines)

Whitelist: a list of URLs or domains that are permitted by a filter

Blacklist: a list of URLs or domains that are not permitted by a filter

How DNS works



- 1) User requests content (by URL or search)
- 2) Server accepts request, passes along to DNS to locate content
- 3) DNS matches request to domain, provides IP address of content
- 4) Path is plotted to content, website is served back to user

How OpenDNS works



OpenDNS



- 1) User requests content (by URL or search)
- 2) Server accepts request, passes along to OpenDNS to locate content
- 3) OpenDNS checks request against the filtering list, then ratifies or blocks the request
- 4) Path is plotted to content, website is served back to user (or not)

How to make OpenDNS work for you (even if you don't want to filter)

- Think about what you'd like to manage with a filter, like the types of content users can reach, sites that infect visitors, or peer-to-peer traffic
- Log into your OpenDNS filter, set up the categories you want to filter, and create a bypass code
- Make additions to the whitelist or blacklist and update the bypass code as necessary



Email (or username):

Password:

Keep me signed in until I sign out

SIGN IN

Choose your filtering level

- Whitelist Only** Enabling this feature will **block all websites** except those listed below under your "Never block" individual domains.
- High** Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters. 26 categories in this group - [View](#) - [Customize](#)
- Moderate** Protects against all adult-related sites and illegal activity. 13 categories in this group - [View](#) - [Customize](#)
- Low** Protects against pornography. 4 categories in this group - [View](#) - [Customize](#)
- None** Nothing blocked.
- Custom** Choose the categories you want to block.

- | | | |
|---|---|--|
| <input type="checkbox"/> Academic Fraud | <input type="checkbox"/> Adult Themes | <input type="checkbox"/> Adware |
| <input type="checkbox"/> Alcohol | <input type="checkbox"/> Auctions | <input type="checkbox"/> Automotive |
| <input type="checkbox"/> Blogs | <input type="checkbox"/> Business Services | <input type="checkbox"/> Chat |
| <input type="checkbox"/> Classifieds | <input type="checkbox"/> Dating | <input type="checkbox"/> Drugs |
| <input type="checkbox"/> Ecommerce/Shopping | <input type="checkbox"/> Educational Institutions | <input type="checkbox"/> File storage |
| <input type="checkbox"/> Financial institutions | <input type="checkbox"/> Forums/Message boards | <input type="checkbox"/> Gambling |
| <input type="checkbox"/> Games | <input type="checkbox"/> German Youth Protection | <input type="checkbox"/> Government |
| <input type="checkbox"/> Hate/Discrimination | <input type="checkbox"/> Health and Fitness | <input type="checkbox"/> Humor |
| <input type="checkbox"/> Instant messaging | <input type="checkbox"/> Jobs/Employment | <input type="checkbox"/> Lingerie/Bikini |
| <input type="checkbox"/> Movies | <input type="checkbox"/> Music | <input type="checkbox"/> News/Media |
| <input type="checkbox"/> Non-profits | <input type="checkbox"/> Nudity | <input type="checkbox"/> P2P/File sharing |
| <input type="checkbox"/> Parked Domains | <input type="checkbox"/> Photo sharing | <input type="checkbox"/> Podcasts |
| <input type="checkbox"/> Politics | <input type="checkbox"/> Pornography | <input type="checkbox"/> Portals |
| <input type="checkbox"/> Proxy/Anonymizer | <input type="checkbox"/> Radio | <input type="checkbox"/> Religious |
| <input type="checkbox"/> Research/Reference | <input type="checkbox"/> Search engines | <input type="checkbox"/> Sexuality |
| <input type="checkbox"/> Social networking | <input type="checkbox"/> Software/Technology | <input type="checkbox"/> Sports |
| <input type="checkbox"/> Tasteless | <input type="checkbox"/> Television | <input type="checkbox"/> Tobacco |
| <input type="checkbox"/> Travel | <input type="checkbox"/> Video sharing | <input type="checkbox"/> Visual search engines |
| <input type="checkbox"/> Weapons | <input type="checkbox"/> Webmail | |

Settings

1 network ▾

- Add/manage networks
- Reverse Memorial Library 169.244.70.72/29

Web Content Filtering

Security

Bypass Blocked Pages

Bypass Blocked Pages

Give users in your organization special permission to access content that is blocked on your network.

Enable/Disable | [Grant permission to a user](#) | [Create a bypass code](#)

Enable block page bypass
When enabled, block pages include a link for users to bypass the block. Only users who are granted permission or have a bypass code can use the link. When disabled, block pages do not show the link even if you have created bypass codes or granted permission to a user.

APPLY

doubleb04645@yahoo.com is allowed to access:

DOMAIN	
. (All domains)	<input type="checkbox"/>

You have 1 active bypass code

CODE	HAS ACCESS TO	EXPIRES	REVOKE
4H565	Domains: . (All domains)	25 days	<input type="checkbox"/>

Note: Patron

REVOKE ACCESS

What else can OpenDNS do for you?

Security

Botnet Protection

Enable botnet protection

Enabling this option protects your hosts and websites from botnets. We continuously update our lists of botnet hosts to keep you protected.

Malware Protection

Enable malware protection

Enabling this option protects your hosts from malware (sources of infection). We're constantly updating our lists in coordination with security vendors.

Internet-Scale Malware/Botnet Protection

Enable basic malware protection

Enabling this feature protects your hosts from types of Internet-scale malware, such as the Microsoft Explorer Zero Day. We recommend you enable this feature.

Phishing Protection

Enable phishing protection

By enabling phishing protection, you'll protect everyone on your network from known phishing sites using the best available information.

Block Page

When blocking content you can choose to redirect to your own internal URL to show users when they visit a blocked site, or you can use our standard block page template. If you want to redirect to your own page and customize the page with more information about what was blocked and why, please visit the [documentation](#).

- No custom block page message**
- Block page with your messages**
- Redirect to your block page URL**

Phishing Block Page

This page is displayed whenever a user visits a suspected or confirmed phishing site. You can use our standard template or redirect to your own internal URL.

- No custom phishing block page message**
- Phishing block page message**
- Redirect to your phishing block page URL**

Malware/Botnet Activity Detected

Need help? Read our [malware FAQ](#).

ACTIVITY	LABEL	IP	STATS	LAST SEEN	HIDE
Malware	Revere Memorial Library	169.244.70.72/29		May 6, 2:32am UTC	

How do I get started with OpenDNS?



Enroll in MSLN with Networkmaine (if you're not already enrolled)!

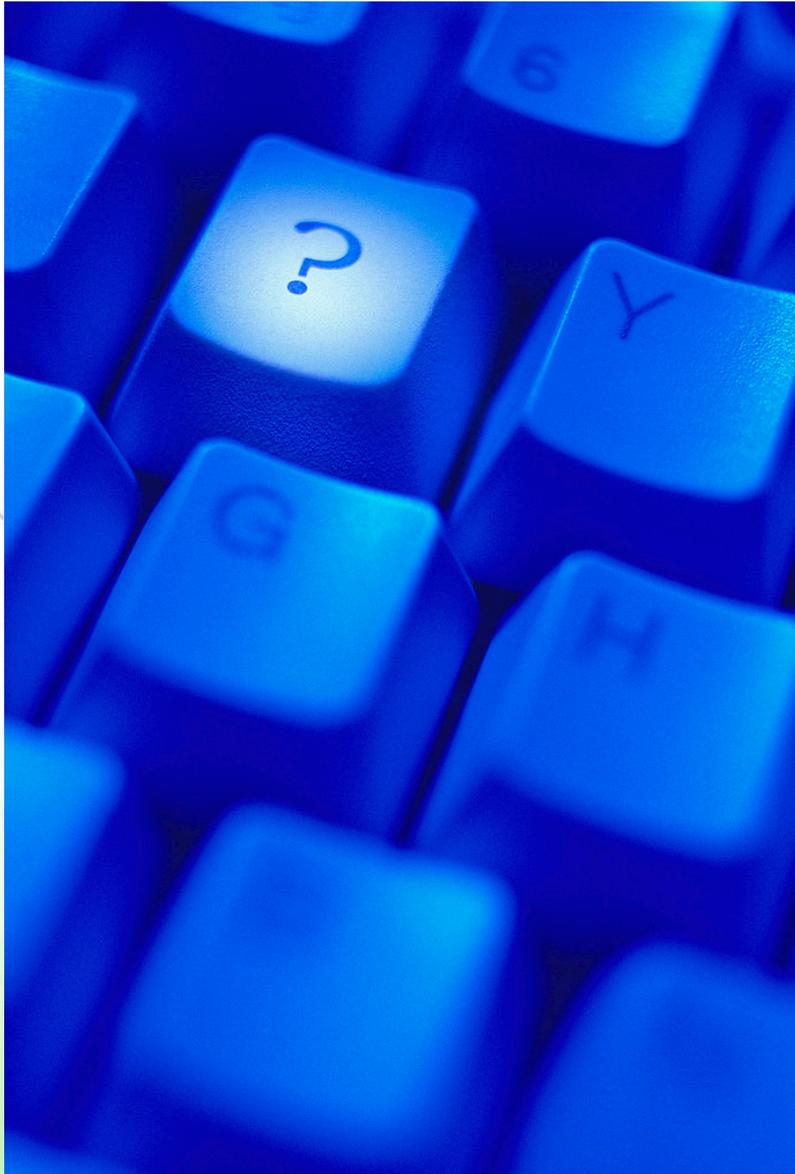


Contact MSLN Support
1-888-FOR-MSLN
(1-888-367-6756)
support.msln.net

OpenDNS

Log in to your OpenDNS filter
at filter.networkmaine.net
and you're done!

Questions? Comments? Cookies?



Participants will receive an email following the presentation inviting them to take a survey. Please help us help you by completing the survey!

Completing the survey will lead you to a web page where you will find additional documents to help you with internet policies and OpenDNS configuration!

**This presentation has been
brought to you by the letters**



Have a great day!

Jared Leadbetter

Jared.Leadbetter@maine.gov

207-287-5620