

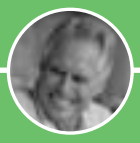

Internet Filter Systems and filtering pupils' access on the Internet

Introduction – what are filtering systems?

Filtering systems prevent or block users access to unsuitable material. When the filtering system is turned on, users cannot open or link to sites that the filtering system recognises as unsuitable. Although a useful tool, filtering systems are not foolproof. They should not replace vigilance or simple common sense from network administrators, teachers or parents.

Filtering content is just one way of making sure that children do not access inappropriate material. Schools need to consider the other ways of ensuring pupils do not have access to inappropriate material. Schools also need to monitor what pupils are logging on to. The schemes of work for ICT include teaching pupils to question the source of web material. Teachers need to equip learners with the skills to become discriminating users of the Internet.

Pupils, staff and parents should sign up to an Acceptable Use Policy (AUP), and there should be clear sanctions if your approach is to be effective. An example of an AUP is contained within this pack.

How do filtering systems work?

The most basic systems have an 'allow' list of sites. Users can only access the list of sites supplied with, and supported by, the system. Access to all other sites is denied. These systems might take the form of a stand-alone Web browser that only allows access to pre-screened safe sites. Walled gardens are the most restrictive type of filtering, providing limited access to the Internet. See the section on 'Walled Gardens' in this pack.

Other systems have 'deny' lists, where users can access any site except those on the system's 'deny' list. These systems are much less restrictive, but the 'deny' list must be updated constantly to be effective, as sites and addresses often change. The decision to include a site on an 'allow' or 'deny' list may be made by the software vendor with little or no input from purchasers. Such decisions can be subjective or controversial in themselves.

Types of filtering systems

Keyword matching/blocking systems:

Keyword matching/blocking is a more flexible filtering technique. The filter analyses downloaded material and blocks any sites containing previously determined unacceptable words or phrases. If the filter finds any unacceptable matches, it will either completely block access to the site or the offending words will be stripped from the page when it is displayed. This can mean that the user is unaware that the filter has altered the viewed page. The list of keywords can often be customised to allow some flexibility in users Internet access or to support different levels of access for different user groups. Unlike 'deny' lists, keyword matching may not be able to prevent Web pages containing undesirable pictures from passing through the filter as they may not contain any text to trigger the filter.

Keyword matching/blocking systems may prevent access to acceptable material because the filter may not be able to differentiate between different contexts and so not distinguish between suitable and unsuitable sites. This is called overblocking. For example, users of some systems might not be able to access information about Middlesex or breast cancer, and filters can have difficulty distinguishing between sites advocating racial intolerance and those which provide support and information for anti-racist groups. However, some filters are able to check the context of words, as well as word occurrences, which helps to rule out overblocking.

Many words that are objectionable in some contexts are perfectly acceptable in others. Find out how "intelligent" the keyword matching/blocking system is - can it distinguish between different word contexts at all? Can you modify its list of objectionable terms to add or delete entries? How straightforward is this?

Many filtering products use a combination of these approaches, offering both 'allow' or 'deny' lists and keyword matching.

While site-blocking systems (see below) require constant updating, keyword matching/blocking systems do not need to be updated quite so frequently; language does not change as rapidly as the Internet. In many ways keyword filtering is a


more dynamic approach to preventing access to undesirable content than site-blocking, with its additional overheads of constant review and updating. However it frequently lacks any context sensitivity, and in isolation is often regarded as a clumsy and poor defence against objectionable material.

Site-blocking systems:
Some filters are able to block at the domain or host level, for example, http://www.becta.org.uk, whilst others can block down to the directory and file level , for example, http://www.becta.org.uk/ technology/faqs/stats.html. This is especially relevant in the case of ISP hosted sites which don't have a "top level domain".

For example you would want a filter to block out access to pornographic sites without blocking access to http://www.website.net/education.

Find out at what level the site-blocking system operates. If possible, try the filter out using domains that carry a mixed bag of information, some of which is objectionable and some of which is not.

Remember that the categories used to identify and group objectionable content are proprietary and are often based on arbitrary, subjective judgements. Apart from the PICS (Platform for Internet Content Selection: http://www.w3.org/PICS/) standards there is very little, if any standardisation for identification and classification of materials across different site-blocking systems. No one rating system has yet been widely adopted by content producers.

Also remember that the pace of change and development on the Internet makes regular update and review essential if a product's proprietary allow and/or deny lists are to be kept up-to-date and effective. Check how frequently lists are updated and also how updates are delivered to you – does the system update itself automatically, or do you have to download and install updates yourself?

Companies' proprietary allow and deny lists are the principal selling points for their products. Suppliers use these lists to differentiate themselves from each other and their lists therefore differ considerably in both approach and coverage. Make sure that as far as possible that suppliers' philosophies, contexts and approaches to categorising inappropriate content do not conflict with your requirements to provide access to appropriate materials. For example, a product aimed at filtering in a workplace, perhaps to avoid off-task "time-wasting" by employees may block a good deal of content relevant to the schools and colleges.

You are unlikely to find a perfect match so ensure that you are able to customise the filter you choose to better meet your needs. For example, does the filter include facilities to make sites that are incorrectly blocked available? How easy is it to change, remove or include individual sites or categories? A site-blocking system that takes days to provide access to an incorrectly-blocked site is likely to cause a great deal of frustration amongst both staff and users.

Keyboard monitoring products:
Keyboard monitoring products check for inappropriate input on the keyboard against a preset list. This technique prevents pupils from using inappropriate search terms. It is best for stopping outgoing information such as credit card numbers and personal information in chat rooms or e-mails.

Protocol-blocking systems:
By restricting access to certain protocols, you can restrict what can be done with your Internet connection. You may wish to deny access to certain types of Internet service, for example to disable access to telnet, ftp, gopher, chat facilities or Usenet. Make sure that the filter you choose supports this functionality if you require it to do so.

Time-related filtering:
ICT facilities that are used at different times by a variety of people for a range of different tasks, (as are common in schools, libraries and lifelong learning establishments), require flexible approaches to filtering. You might therefore wish to limit or restrict Internet access by time of day. For example, very restrictive filtering might be fine for use by primary children, but is likely to be inappropriate for out-of-hours use of computing facilities by older children or adults. You may wish to limit access to certain services that make large demands on your network at certain peak times. Make sure the filter can differentiate in this way, if this is one of your requirements.

Client- and server-based filtering systems:
Client-based filters have to be installed and maintained on each individual computer or workstation used to access the Internet. These systems are prone to tampering and are more difficult to keep current. Server-based filters are installed either at a central location maintained by a network administrator at the institution or remotely where they are administered by an ISP. In this second instance, filtering is one of the services available to subscribers to the ISP. This sort of filtering is effective throughout the entire network and is not prone to tampering at individual machines. Each client workstation is set up to access the Internet via the server. Some products allow the network administrator to keep a record of the numbers and locations of any attempted undesirable accesses.


Managed Service Providers:
Filtering facilities to restrict access to inappropriate material published on the Internet are provided by each NGfL Managed Service supplier. Filtering methods and the extent to which filtering is under the institution's control will vary. Ask how filtering mechanisms are administered within the services you are offered and make sure that they are sufficiently flexible to accommodate all your requirements. For example, you may wish to heavily safeguard very young children's Internet use, whereas older pupils or adults using the same network may find such safeguards unduly restrictive.

Further information:
The Parents Information Network (PIN) was commissioned by the Department for Education and Employment (DfEE) to undertake the impartial evaluation of Internet filtering software programs. See, http://www.pin.org.uk/filtering/index.htm

First steps and things to think about…

- It is important that you consider your options carefully. Think about what you want to happen when a user tries to access a blocked site or send an inappropriate e-mail. Find out how filters actually handle sites and content that they block. What do users see when the filter is activated by a request for banned material? For example, if a keyword matching/ blocking system identifies a match, it might either not display the offending page or e-mail at all, or display it but with the offending content obscured or stripped out. In extreme cases, filters can shut down the browser or lock the computer when a user tries to access banned content, sending an alerting e-mail to the system administrator in the process.

- Remember that all schools have a responsibility to filter both access at school and any access pupils are given as part of home-school links. Becta has defined a functional specification that all NGfL Certified Managed Services must meet. It includes internet access with filtering services that help to prevent access to undesirable material. For more information visit: http://www.managedservices.ngfl.gov.uk/2/

- Filtering is an effective tool, but it is important to remember that no filtering software is foolproof and should be combined with the full range of management measures set out in the Superhighway Safety guidelines.

- See the section called 'Checklist for evaluating filtering systems' to help you to evaluate the filtering products that will work for you.

- See the section called 'Running filtering systems' for a variety of locations from which you can run filtering systems. For schools, services provided at ISP or server level provide greater security and less chance of individuals tampering with settings, and are easier and more economical to manage.

- Different groups of users and machines may require different filters, and the importance of customisation facilities and the ease with which filtering systems can be administered and tailored to individual needs should be considered. However, there are a number of overarching implementation and administrative issues to consider, both when filters are installed on individual PCs and especially when they are deployed across a network with a wide range of user groups and client machines. See the section 'Different users may require different filters' for more information.

Checklist for evaluating filtering products

1. Identify your requirements for a filtering system as accurately and as comprehensively as possible. The descriptions of different filtering techniques and the advice contained within this information pack will help you with this.

2. Review your current network infrastructure and Internet connectivity to ensure that you choose a filter that will work in your particular environment.

3. Examine filtering products and systems in the light of those requirements to find the best match.

4. Consider if the filter can meet all of your requirements and, if so, how easy and straightforward it is to implement and tailor to your needs. Of paramount importance at the client level is the ease with which the filter can be bypassed or disabled. Make sure that the filter is secure, especially on machines that are often used without supervision.

5. Consider where and when to filter.

Running filtering systems

Filtering systems can be installed and run from a variety of locations, ranging from a single user PC to Internet service providers and beyond:

1. On individual PCs. A number of filtering tools are designed to run on stand-alone PCs. This approach may be appropriate for the home environment in that it allows parents to configure Internet access as they choose. However, it is much less appropriate for

deployment across a network, as updates and reconfigurations will have to be carried out at each client machine rather than from a central location. Another disadvantage of client-based filtering is that it may be possible for users to reconfigure or even disable the filter themselves, although many products include safeguards against such tampering.

2. At LAN or local proxy level. Here the filter is installed across a network so that it covers all clients on the network, intercepting all web page requests and e-mail traffic. This means that all configurations and updates are carried out centrally making system administration and updating much easier. Such central installations are also harder for individuals to tamper with at both local and remote level.

3. Using a remote proxy server. In this instance users configure their Internet connectivity so that all Internet traffic and requests pass through a proxy server. This server, which may be located geographically far from the institutions local area network, hosts the filtering or content access management system.

4. By the Internet Service Provider (ISP). A number of ISPs provide services based around content specifically for children, alongside providing filtered Internet access. Some will also restrict access to chat rooms, newsgroups or other types of Internet services as appropriate.

5. Search engines and web sites. Some search engines only return hits that are appropriate for children whilst some web sites function as portals of links especially designed for children to explore. This method works by guiding users to appropriate content rather than by denying access to unsuitable materials and is therefore somewhat removed from the approaches described above, but is still worth considering.

Examples of good practice can be found on the Superhighway Safety web site.

Different groups may require different filters

1. You may wish to provide younger users with more restricted access whilst allowing greater privileges to older users. Similarly, you may need your filtering system to distinguish between different client machines on your network.

2. Workstations in a more public location that are often used without supervision from school, college or library staff might need more restrictive filtering than workstations that are only used under supervision.

3. Levels of access supported by filters can vary greatly. Some filters are basically on or off whilst others allow specific configurations for different workstations at individual or group level.

4. Remember that filters are far from being a fit and forget solution to the problem of preventing access to undesirable Internet content. Just like your network users, filters require regular management, administration, maintenance, updating and review if they are to be effective.

5. Make sure that both you and your staff have sufficient time, expertise and resources to manage and maintain any solution you implement.

6. Whilst devolving filtering responsibilities to a third party such as an ISP has advantages in terms of reducing system administration tasks, the trade-off is potentially reduced control over filtering methodologies. It is important to strike a balance between devolving responsibility and maintaining flexibility and control over what and how filtering is carried out.

Useful Links:

The following papers and web sites provide further information that will help you assess filtering products and technologies.

1. AT&T Technology Inventory: A Catalog of Tools that Support Parents' Ability to Choose Online Content Appropriate for their Children

This document provides an inventory of technologies that support parents' ability to choose content appropriate for their children, or address online personal safety issues affecting children. Whilst published some time ago (first in 1997 and subsequently revised in Sept 1998) it provides a useful overview of different filtering approaches and technologies. It is downloadable from http://www.research.att.com/projects/tech4kids/

2. Safeguarding the Wired Schoolhouse: A Briefing Paper on School District Options for Providing Access to Appropriate Internet Content

Published in October 2000 by the US Consortium for School Networking (COSN), this white paper outlines issues to consider when developing Internet access policies for schools. It is available online at: http://www.safewiredschools.org/publications.html

3. Blocking Content on the Internet: a Technical Perspective

This paper, published by the Australian National Office for the Information Economy (NOIE) in June 1998, is more technical in content than the previous two papers but is nevertheless worth a look. It is available at: http://www.noie.gov.au/projects/consumer/content_regulation

/blocking1/blocking.htm and as a downloadable RTF file at http://www.noie.gov.au/publications/publications.htm

4. GetNetWise

This site, available at http://www.getnetwise.org, was set up by US Internet industry corporations and public interest organisations to "help ensure that families have safe, constructive, and educational or entertaining online experiences". It includes links to more than 140 filtering tools, alongside advice to help you choose products best suited to your requirements.

5. Commission on Online Child Protection: Report to Congress

The Commission on Online Child Protection was set up when the US Congress passed the Child Online Protection Act (COPA) in October 1998 as a temporary commission of 19 members to study "various technological tools and methods for protecting minors from material that is harmful to minors."

Among the methods Congress asked the COPA Commission to examine were:

- a common resource for parents to use to help protect minors (such as a 'one-click-away' resource)
- filtering or blocking software or services;
- labelling or rating systems;
- age verification systems;
- the establishment of a domain name for posting any material that is harmful to minors; and
- any other existing or proposed technologies or methods for reducing access by minors to such material.

The Commission released its final report to Congress in October 2000, which is available online as a PDF file at http://www.copacommission.org/report/

6. US National Research Council Project on Tools and Strategies for Protecting Kids from Pornography and their Applicability to Other Inappropriate Internet Content

The American National Research Council is undertaking this project at the request of the US Congress to examine tools and strategies for protecting kids from pornography and their applicability to other inappropriate Internet content. Work is currently ongoing; further details are available at: http://www.nas.edu/itas

7. EU Safer Internet Action Plan

The European Union is coordinating an Action plan to promote safer use of the Internet. Projects include a European network of hotlines to allow the reporting of illegal Internet content, investigation of filtering and rating systems and raising awareness of both the Internet's potential and dangers. Full details are available at: http://europa.eu.int/ISPO/iap/

Examples of filtering software packages

AT Kids Browser is a multimedia web browser, which provides an educational filtered environment for children to surf the Internet. http://www.winshare.com/mkbindex.htm

The Bair Filtering System contains both an image and text recognition filter. Unsuitable images are removed from the page before they reach the browser. http://www.thebair.com/

The Bess Internet Filtering Service operates at the server, or network level, and provides filtering for every computer on the network. http://www.n2h2.com/solutions/school/school_products.html

Chaperon 2000 (C2K) is an Internet filtering program, which can notify a school when a child has attempted to access inappropriate material. http://www.edu-tec.com/

ChiBrow is a Web browser designed for children, and which allows parents to define where their child can go. http://www.chibrow.com/

Cyber Patrol is an Internet access management tool, aimed at parents and teachers, and used to control children's Internet access. It comes loaded with a list of researched Internet sites that contain potentially unsuitable material. http://www.cyberpatrol.co.uk/

Cyber Sentinel can take screen captures of user activity, and monitors both on- and off-line use. http://www.securitysoft.com/

CYBERsitter allows parents to limit children's access to unsuitable Internet material. It filters and blocks adult-orientated material, graphics and language from Internet newsgroups, chat areas, World Wide Web pages and e-mail. http://www.solidoak.com/

Cyber Snoop places the emphasis on teaching responsible Internet use through supervision and communication. Cyber Snoop educates users to make positive choices on the Internet. http://www.cyber-snoop.com

FamilyConnect is an Internet filtering service that blocks illegal web sites while still giving access to the millions of other Web pages on the Internet. http://www.pornblocker.com/

FamilyConnect 2000 offers continuous monitoring and protection even if you add or remove browsers or change ISPs. http://www.cleansurf.com/

I-Gear for Education offers a content management application designed specifically for schools. Supports roaming users by allowing bookmarks and history to follow the user regardless of the computer being used.
http://www.symantec.com/sabu/igear/igear_educ/

IF-NOT, the Internet filter for Windows, monitors, filters, analyses and logs Internet access. http://www.turnercom.com/ifdir.html

KidDesk Internet Safe lets parents choose which web sites, CD and software programs children can access from a personalised desktop. Children can navigate appropriate sites, record messages or leave notes in a message centre.
http://www.edmark.com/prod/kdis/

Klik1 provides reference links to companies offering child surfing safety software and organisations offering advice on child Internet safety.
http://klik1.home.att.net/kids/kparents.htm

N2H2 provides Internet filtering technology to schools in the US, Canada, the UK and Australia.
http://www.n2h2.com/solutions/school/school_products.html

Net Nanny acts as an invisible monitor between the Internet and the user, screening out pre-determined, user-defined sites, words and content. http://www.netnanny.com/

NetSweeper offers a range of Internet filtering products to the USA, Canada, the UK and Latin America. It uses a global filtering selection in multiple languages and can be used in educational institutions, libraries and corporations. Its filtering system is content-based and filters sites deemed illegal, offensive, non-productive, or contrary to school or work related activities.
http://www.net-sweeper.com/english/

Planetweb Parental Control allows parents and teachers to filter access using a 'white list' (each web site to which it allows access has been reviewed and is part of a database).
http://www.planetweb.com/products/web/pc.html

PureSight Education is an Internet Access Control (IAC) tool designed specifically for use in schools, libraries, and other public access sites. It screens and analyses all Internet traffic, controls access to inappropriate material, monitors and reports on which sites have been visited, and selectively blocks access according to user and age group. http://www.puresight.net/Products/PureSightEducationDescription.htm

RM SafetyNet Plus is a powerful web-based Internet filtering system, which enables schools to directly specify which web sites their users can browse or search for. The school builds individual filtering lists, which are accessed via an administrative web site. This means that there is no requirement for any additional hardware or software at the school. http://www.rm.com/safetynet

SafeKids.Com includes a chart listing Internet filtering products and their features and offers access to the product web sites.
http://www.safekids.com/

SafeSurf has developed and implemented an Internet Rating Standard that brings together parents, teachers, providers, publishers and developers. Suitable sites are marked with the 'SafeSurf' wave. http://www.safesurf.com/

SurfControl is a content filtering solution which blocks topics across 39 categories of sexually explicit material, violence and hate speech, gambling, illicit drugs and alcohol.
http://www.surfcontrol.com

We-Blocker is a filtering product, which enables parents to create accounts for each family member, with restricted access to particular categories of material.
http://www.we-blocker.com/

Which On-Line published a review of Internet filtering products in May 2000. http://www.which.net

X-STOP is a family of technology-based Internet blocking products, offering direct access blocking (DAB). It uses automated search technology to seek out, identify and block over 96% of all pornographic sites on the Internet.
http://www.xstop.com/

Various computer magazines regularly review Internet filtering products. It is advisable to refer to the most recent edition.