



BMAS Guidance Notes

**Content Filtering in
Education.**

BMAS

Tech/BMAS/005

Contents

1.0 Overview

2.0 Considerations

3.0 Where to run a content filtering solution

4.0 How content filtering systems work

4.1 Basic content filtering methods

4.2 Other more sophisticated methods

4.3 Filtering of e-mail and other applications

5.0 Findings from the FE sector

6.0 Considerations and recommendations

References

Trademarks

Introduction

This document is compiled from the experiences of a number of Regional Support Centre (RSC) and Further Education (FE) college staff, and the BMAS team. It offers an overview of the technical solutions available and outlines which products are widely used in education as well as any common problems that are encountered by IT staff. It also assesses the facilities and advice provided by various government departments and outlines recommendations received from the community.

1.0 Overview

Content filtering is the process of removing unwanted files and content, or preventing access to certain websites, for the protection of systems and users from harmful or offensive material and to protect systems from security risks.

In an educational environment with many users, some or all of whom may be under 18, careful consideration must be given to the blocking of potentially harmful or offensive material. There are many different solutions available today that can help you achieve this, all of which have varying tools and modus operandi. This document will help in assessing your needs and requirements from a content filtering solution based on users' profiles, computer systems, available time and budget.

It is important to remember that any content filtering system should be flexible enough to cope with the demands of a wide ranging user set, where a great variety of subject matter may be taught. An over zealous filtering system can be as ineffective as an inadequate solution.

2.0 Considerations

Content filtering is a complex issue with a myriad of solutions using many techniques for a very diverse audience.

It is therefore easy to see how many find this subject rather daunting and indeed there are no hard and fast rules. Indeed the best way to implement an effective content filtering solution is to primarily assess the needs of your organisation based on the following:

- **Platform** - A multi-platform environment requiring a cross platform solution will have a stronger influence if you decide to install a content filtering solution on a per machine basis (see below)
- **User groups** - If your organisation offers a variety of courses to a range of different users you will need an adaptable filtering system that can change according to different times of the day or different users.
- **What you want to filter?** - Do you only want to filter standard web traffic (HTML pages etc.) or a range of applications such as e-mail, File Transfer Protocol (FTP), Usenet, chat, peer-to-peer file sharing etc.
- **Timed access** - This may be a consideration with a broad range of users requiring access at different times of the day. See the point about User Groups above.
- **Acceptable Use Policy (AUP)**- A content filtering system with relevant categories, banned file formats and URLs etc. should be incorporated into an AUP. If no policy exists it is strongly advised that the organisation draw up such guidelines.

- **Budget** - Some advanced or managed resources can be very expensive, although there are so many products available including open source™ solutions, that an organisation should be able to find a viable solution to match its needs.
- **IT staff Expertise** - Content filtering systems must be assessed on the technical management requirements. Some content filtering solutions are highly complex with a number of variables that need regularly configuring. Open source solutions can save money but may not be suitable for those who have little open source knowledge.
- **IT staff resource** - The very nature of content filtering solutions means that in order to be effective they must be regularly updated and maintained. This is a very important factor to consider before implementation.
- **Whether a managed resource may be a beneficial option** - Following on from the point above, when staff time is at a premium, managed resources may be an attractive solution although this must be balanced against budgetary requirements.

Once the organisation has considered the above options, it should then assess the various methods of filtering in order to ascertain which is the most appropriate solution.

A good guide through the myriad of options available for content filtering solutions is available on the Department for Education and Skills (DfES) website.

<http://safety.ngfl.gov.uk/schools/>

Note that information on this website is aimed at schools although much of the information and considerations are applicable to HE (Higher Education) and in particular Further Education (FE) colleges.

The BMAS page on 'In Depth Filtering Resources' also lists in detail those filtering products that are popular in UK HE organisations:

http://www.bmas.ja.net/content_filtering/more_resources.html

3.0 Where to run a content filtering solution

There are 3 areas where content filtering solutions can be implemented:

- on a per PC basis - for an organisation of any size this solution is probably not a viable option from a cost and maintenance point of view. Client systems are also vulnerable to tampering;
- on a server basis - a much more manageable solution for many medium to large organisations, and in many cases a more cost effective solution. Also reduces the risk of tampering;
- at Internet Service Provider (ISP) or managed service basis - leaves the IT staff free of the responsibility of maintaining the system although price may be an obstacle. The National Grid for Learning (NGfL) website has a list of recommended suppliers, some of whom can offer managed services. Please see: <http://www.ngfl.gov.uk/>

4.0 How content filtering systems work

As previously stated there are many different methods of content filtering with solutions using one, or a combination of methods. In order to get the best from a content filtering solution you should compare the different methods of filtering, how easy it is to upgrade the system to incorporate new items that need to be blocked or accessed, how often updates are required, and consider factors such as how and if customisation can be achieved etc.

4.1 Basic content filtering methods

Allow and deny lists - Basic content filtering systems work on one of two principles, either an 'allow list' or a 'deny list':

- **Allow lists** only permit users to access a list of sites supplied with the filtering system, thus ensuring a very restrictive form of filtering;
- **Deny lists** permit users to access any site other than those identified in the systems 'prevented' list. Deny lists, whilst being less restrictive than allow lists, require much more maintenance to remain effective.

4.2 Sophisticated methods

- **Site blocking** - Levels of sophistication vary widely with site blocking systems, with domain and host level blocking being standard place and some systems being able to block down to directory and file levels. Organisations should consider not only the level of filtering that they require, but also the categories used by content filtering systems to determine questionable content. These categories are often predefined by manufacturers although some can be added to and further edited by users. As categories change and are redefined, so they often need to be updated. Therefore consideration must be given to whether this is done by an automatic process or by regular manual updates which can be time consuming.
- **Keyword matching or blocking** - Utilises a predetermined list of unacceptable words or phrases, then scans any downloaded material for matches to the list. When a match is found access can either be completely blocked or the offending words or phrases can be stripped out of the web page. Keyword blocking often does not need such regular updating as allow and deny lists, and can be customised, although be aware that on its own, keyword matching or blocking can not filter offensive images. Weigh up how adaptable and intelligent the keyword matching is, i.e. can their system tell when words are used in a different context? This is an especially important consideration for FE and HE where a wide range of subjects may be taught resulting in the real possibility of different words being used in a different context.

4.3 Filtering of e-mail and other applications

- **Keyboard monitoring** - This method can check keyboard input against a predetermined list, assessing inappropriate entries. It is used for e-mail and chat room filtering.

- **Protocol blocking systems** - These systems are also useful for overall network maintenance and monitoring as 'illegal' bandwidth consuming traffic can be blocked, resulting in the release of bandwidth resources and a reduced security risk. Access to FTP, Usenet, chat facilities and MP3 files can all be restricted.

5.0 Findings from the FE sector

The following summation has been constructed out of the findings of a small-scale questionnaire sent to several RSCs in the UK. (Thanks in particular to the RSC North West who very kindly collated our e-mail questions into a printed questionnaire. Thanks also to RSC London for their prompt reply.)

The community was asked the following questions:

- What content filtering solutions do you use?
- Does using a content filtering solution cause a heavy maintenance burden?
- Who is responsible for maintenance of the content filtering system?
- Have you experienced problems balancing the need for filtering for minors against freedom of information for all?
- Is the expense of the software an issue?

What content filtering solutions do you use?

Approximately 66% of organisations used proprietary systems, mainly Microsoft® based, with packages such as Bess, CyberPatrol® and WebSense proving to be the most popular. Some organisations also used filtering systems inherent in their web server software such as Microsoft® Proxy and Internet Security and Acceleration (ISA) server.

Thirty-three percent of those interviewed used Linux® based systems, some of which utilised custom-made filter lists.

Does using a filtering system cause a heavy maintenance burden?

42% stated that using a filtering system caused a moderate amount of maintenance.

42% stated that using a filtering system did not cause them a maintenance burden.

14% stated that using a filtering system did cause them quite a maintenance burden.

Who is responsible for maintenance of the content filtering system?

All reported that the organisation's IT or Computer Services Department was responsible for maintenance of content filtering solutions. Some organisations reported that they collaborated with other departments and staff regarding the updating of filtering lists and categories. Some had implemented their own web forms that could be completed by staff to alert the IT department to additional or current sites and categories that needed adding or editing, with web form results being verified by the IT department.

Have you experienced problems balancing the need for filtering for minors against freedom of information for all?

66% said that they had experienced difficulty balancing filtering with freedom of information for all.

33% said that they had not experienced any difficulty in this regard. The creation of

effective usage policies appears to have helped as well as the use of software that is aimed more specifically at the education market.

Is the expense of the software an issue?

85% of those questioned stated that software expense was an issue
15 % declined to answer.

6.0 Considerations and Recommendations

It is recommended that the following are considered when planning to implement content filtering. Consult section 2 of this document

- Decide where best to install a content filtering system, either on a per PC basis, server basis, or as a managed solution. For most education organisations a server-based system is probably the best solution for licensing, maintenance and security reasons.
- for a very useful guide to some of the many solutions available see the NGfL matrix at:

<http://safety.ngfl.gov.uk/schools/>

See also the BMAS guide to content filtering resources for a comprehensive overview to some of the most popular content filtering solutions available in the UK today:

http://www.bmas.ja.net/content_filtering/more_resources.html

- Read 'How content filtering systems work' Section 4 of this document and assess what approach best suits your needs by taking into consideration staff experience, maintenance required, ease of update, standard / editability of categories etc.
- Our findings from a small survey of FE colleges would seem to indicate that better results are in fact derived from those solutions aimed at the education sector.
- Compare content filtering solutions with budget requirements and check for any update costs that may be required on a regular basis such as category and filter updates.
- Check responsibility for maintenance of filter lists and/or filter categories with the manufacturer, i.e. are updates automatic or manual?
- Check whether predefined lists and categories can be edited by your organisation.
- Review your organisational AUP and incorporate content filtering into the policy.
- Make staff aware of content filtering systems and consider how best to obtain staff recommendations for unacceptable content.
- Bandwidth may be released by filtering illegal traffic such as peer-to-peer file sharing. This can be achieved by a number of methods both on a policy level and through hardware and software solutions.

References

<http://www.ja.net/documents/index.html> - JANET guide to content filtering in education

<http://safety.ngfl.gov.uk/schools/> - NGfL guide to filtering in schools with useful information particularly for colleges. This site shows the Matrix which can help organisations select content filtering solutions by feature.

http://www.bmas.ja.net/content_filtering/more_resources.html - The BMAS overview of popular content filtering solutions used in UK education and research.

Trademarks

CyberPatrol is a trademark of SurfControl plc and is registered in certain jurisdictions

The term 'Linux' is a registered trademark of Linus Torvalds, the original author of the Linux Kernel.

Microsoft is a registered trademark of the Microsoft Corporation in the United States and/or other countries.

BMAS, Manchester Computing,
Kilburn Building, University of Manchester
M13 9PL

Tel: (0161) 2756008 / (0161) 2757195

Fax: (0161) 2756040

Email: support@bmas.ja.net

BMAS is a JANET Service

JANET®, SuperJANET®, and UKERNA® are registered trademarks of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association, trading as UKERNA, is the registered user of these trademarks.

JANET is funded by the Joint Information Systems Committee (JISC)

© The JNT Association 2003