# Web Filtering for Schools

## The Requirement for Differentiated Filtering.

### Introduction

Schools' Internet filtering requirements are complex, encompassing not only the changing needs of children as they develop but also those of staff preparing lesson materials. Schools must both safeguard users and provide access to the broad spectrum of material available online in a way that supports children's learning as fully as possible.

At the same time, it is important to educate all users (both children and staff) on the importance of safe and appropriate online behaviour, ensuring they are properly equipped to use the Internet on devices and in locations where the safeguards provided in schools do not apply.

Studies by Ofsted and psychologist and child safety expert Tanya Byron (commissioned by the Department for Children, Schools and Families) both focussed on the importance of teaching children to manage risk in this area, empowering them to become confident and safe users of the Internet. The Byron Review drew an analogy between learning about being safe online and learning about the dangers of water: we do not just teach children that water can be dangerous, we also teach them how to swim so they can enjoy water safely.

This information sheet describes the technical and policy approaches taken by Regional Broadband Consortia (RBCs) and local authorities to ensure schools' online environments support learning, keep people safe and promote the development of the skills necessary for safe and appropriate behaviour online.

While this information sheet is intended for a technical audience, it may also be of interest to readers with a strategic responsibility for internet access in schools.

## The Background

Two important reports have reflected upon the use of the internet in schools and, in part, make reference to filtering issues: the Ofsted Report The Safe Use of New Technologies (2009) and Safer Children in a Digital World, also known as the Byron Review (2008).

The Ofsted report makes a distinction between locked down and managed systems. In a locked down system, "almost every site has to be unbarred before a pupil can use it". In contrast, managed systems "also have inaccessible sites, [but] there are fewer of them". The exact nature of the distinction between locked down and managed systems is not explicitly defined, but could be characterised as the difference between blocking all sites unless previously approved (establishing what is sometimes referred to as a walled garden) and a presumption to allow access unless there is clear reason for a site to be blocked.

The Ofsted report makes very clear that the managed approach is to be preferred, with the explicit recommendation that schools should "manage the transition from locked down systems to more managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school". This recommendation also forms part of Ofsted's September 2012 Inspecting e-safety briefing for inspectors.

The Byron Review expressed a similar view:

> *"There is a general social consensus, reflected in our approach to film and television content, that explicit pornography and violent material such as videos of executions is not suitable for children. However, there is no such consensus about material such as non-pornographic nudity, violence or death in an educational context (such as information about wars or the holocaust) and the websites of extremist political parties. Similarly, many parents would wish to stop young children from stumbling across such material, but would be keen for their children to see such material when they are older teenagers or when it can be put in an appropriate context."*

It also acknowledged the importance of differentiating access across user groups:

> *"The decision about what constitutes 'inappropriate content' can be highly subjective. What one person views as harmful, another might find offensive, whilst yet another might see it as an important, empowering learning experience for their child; and this view is likely to change depending on the age of the child. An example of this might be a sex education website. In consequence, any attempt to block content which falls into these grey areas would leave some*

> *parents unhappy that the system was either too restrictive or not restrictive enough ...”*

While the Byron Review was mainly concerned with internet access and filtering in the home, these same issues – of inadvertent access to inappropriate material and the important of age differentiation in what is considered to be inappropriate – are even more applicable in schools, where pupils from 5-18 as well as staff are using the Internet. Any filtering system used must be able to cater for the diverse needs of these different groups of users.

## Particular Needs fo Staff Users

Teaching staff have very particular needs in relation to web filtering systems. For example, if the same filtering rules apply to staff as to their students, staff will be unable to use their professional judgement to evaluate whether a blocked site should in fact be allowed. Staff may feel that a particular site is suitable for sixth form students but not for others: but how are they to make this judgement if the site is blocked not only to all students but staff as well? This is not to say that staff should have completely unfiltered internet access; rather, there should be a presumption of allowing staff access to sites which may fall within the grey areas noted in the Byron Review.

Staff need to research their subject and may want to use certain sites which are, for whatever reason, blocked to students. This is independent of whether they may subsequently want their students to visit the site. To use the example cited in the Byron Review above, a history teacher may want access to a site about the Holocaust to gather information and images for a classroom lesson. The teacher may, indeed, feel that the site is not suitable for student viewing, but they still need access themselves in order to contextualize the information it contains.

Similarly, there are clearly situations where it makes sense for staff to be able to show to a whole class parts of a particular site that they would not want pupils to be able to use unsupervised. For example, there are many very useful videos on YouTube that staff may want to show to a class. But YouTube also contains a vast quantity of very inappropriate material so it is generally blocked to students.

## Requirements

Taking these two reports into consideration allows us to be able to specify in broad outline the facilities required for a school web filtering system:

1. The general ethos of the system should be to allow a site unless there is some reason to block it. The reason may be a generic one (i.e. block all online games sites) or very specific (e.g. this site contains language which is not suitable for Year 9 students). The key is that there is a defined policy of when a site is, and is not, allowed.

2. It must be possible to have age differentiated filtering rules for students. A particular site (or even a particular page within a site) may be considered suitable for pupils in the sixth form but not those in Year 9 or younger. An example could be a site designed for lawyers or law students where criminal cases are discussed in great details with crime scene photographs. This would clearly be distressing if viewed by a primary school pupil but could provide valuable research to a sixth former studying A-level psychology or law.

3. There must be a set of filtering rules designed specifically for staff use.

These requirements are dependent upon effective user education being in place in the school for staff and pupils, along with a clearly articulated policy on how any breach of the rules or any disclosed threat to pupil or staff will be handled. The first of the items above is about the way the lists are managed, while the second two are concerned with how these lists are applied to a particular user. In particular the filtering system must be able to apply different filtering rules (rulesets) to different populations of users within each school. As an absolute minimum, each school needs to be able to access two contrasting rulesets: one for its students and one for its staff. For a more flexible approach and to allow for age differentiation within the school a wider range of rulesets would be preferable. For example, a secondary school could use one ruleset for the lower school, another for GCSE students, another for sixth formers and another for staff.

Some schools also like to have the ability to restrict internet access further as a disciplinary measure: rulesets that deny all internet access or allow only very restricted access (a “walled garden”) are seen as very useful in this context.

## Architectural Issues

Given this need for multiple rulesets some architectural issues need to be addressed.

The first, and perhaps most fundamental, is that filtering must take place before caching. A web cache stores copies of documents passing through it; subsequent requests may be satisfied from the cache if certain conditions are met, reducing the load on the institution's broadband connection and improving performance.

Filtering must take place before caching because both the user and client workstation identity are unavailable to the filtering service when the web request has been passed through a cache, meaning only a single ruleset can be applied. Also, due to the caching mechanism, some 25-35% of all requests will never be examined by the upstream filtering system as they will be met from the local cache. That is to say, the result of a single web request to the filtering system will often be sent to multiple users. Due to these factors the possibility of any age discrimination is lost if any caching is implemented before the filtering.

So, if caching at the school is required (e.g. to increase performance on constrained bandwidth), then the filtering needs to be implemented in the school, either on the cache hardware or via a separate filtering service accessed prior to the cache.

It is also possible to have this age differentiated filtering when the filtering is provided as a central, local authority wide service.  All that is required is some way of directing a user's browser to the filtering system in such a way that the ruleset to be used can be determined. There are a variety of ways in which this can be achieved:

1. using multiple ports on a common proxy IP with each port relating to a specific ruleset;

2. using multiple IP addresses for the service where each IP provides a specific ruleset;

3. using a LA wide authentication system to assign users to rulesets at login.

In the first two cases the school's own network system would be used (via group policies in AD for example) to provide the appropriate proxy details to each user's browser.

All the methods above provide a common collection of rulesets and URL lists for the sites using the filtering system. It is also possible to provide a more tailored service where the schools themselves have some control over the filter rulesets and lists. In architectural terms, this can be provided either as a central service or via local servers. A central service could be provided as, for example, a farm of virtual filter servers hosted on a central array of physical servers with all the advantages of central management. Such an architecture would allow each school to have direct access to the management of the filtering service they receive (via a web interface) in order to make specific changes to the rulesets and lists without affecting other schools in the authority. The disadvantage of this remotely provided local service is that caching cannot be done locally: each browser request must be handled by the remote virtual server before any caching can take place.

Using a local server (either real or virtual) has the added advantage of allowing caching to be done within the school which reduces the bandwidth requirements.

There are several critical advantages to using a local service (whether provided locally or remotely):

1. By linking to the local directory services the filtering server can be configured to use an appropriate ruleset for each user, add usernames into the filter logs and give school staff access to reports of user activity.

2. The url lists can be adjusted to more closely reflect the circumstances and ethos of a particular school rather than relying on a "one size fits all" set of rules and lists managed centrally.

3. Any changes to the lists can be made instantly and without reference to a third party who may, or may not, want to make the change for all the connected schools.

## The role of local authorities and RBCs: brokering solutions

The complexity of schools' filtering requirements underlines the importance of local authorities and RBCs in brokering effective solutions for schools.

RBCs and local authorities understand and can aggregate their customers' requirements, meeting them using the broader market to deploy technologies that provide the best balance of capability, performance and cost in particular areas. The technical expertise and buying power of RBCs and local authorities acting on behalf of schools enables the effective and timely updating of services to take advantage of new technical opportunities. A thorough understanding of product and technology roadmaps and lifecycles is key to a strategic approach to provision, keeping pace with continually increasing requirements for speed and performance.

RBCs and local authorities have a successful track record in this regard, having grasped the nettle of complex provision to deliver high performance, cost effective, scalable infrastructure and services for schools over many years.

Ofsted's September 2012 *Inspecting e-safety briefing for inspectors* identifies school Internet provision via a "recognised Internet Service Provider or RBC together with age related filtering that is actively monitored" as a key feature of "good and outstanding practice".

The expertise within RBCs and local authorities means that technologies like filtering can be deployed in a way that supports schools as fully as possible, both in terms of safeguarding users and enabling them to develop the skills they need to participate in the UK's digital future.

## Sources of further advice

NEN: e-safety
https://www.nen.gov.uk/advice-for-schools/online-safety/

CLEO: e-safety
http://www.cleo.net.uk/index.php?category_id=591

E2BN: e-safety
https://www.e2bn.org/cms/e-safety/e-safety

LGfL: e-safety
https://www.lgfl.net/online-safety/

South East Grid for Learning: e-safety microsite
https://www.segfl.org.uk/online-safety/

South West Grid for Learning: Staying Safe
https://swgfl.org.uk/online-safety/

WMnet: e-safety
http://www.wmnet.org.uk/index.php?option=com_content&view=category&id=13&Itemid=142