WARRINGTON
Borough Council

Web Filtering for Schools – WBC IT Statement February 2023

Web filtering is a solution that controls what information users can and cannot access over the Internet.

This update is provided to help schools and their stakeholders understand the current solution in place for Schools that purchase WBC's Network Service.

Statutory Guidance on 'Appropriate' Web Filtering

There is statutory guidance on what the UK law deems appropriate for protection of children with relation to internet access:

The Revised Prevent Duty guidance for England and Wales: (Link)

> *"…to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering…"*

The DfE's Keeping Children Safe in Education 2022 guidance: (Link)

> "141. Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs verses safeguarding risks."
>
> "142. The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty."

Ofsted's School Inspection Handbook 2022

> *"28. We do not require schools to:*
>
> *use a digital platform to monitor pupils' internet use, and we do not specify how these platforms should operate''*

The Council's Web Filtering Service

The Council's service is provided as part of the Network Service using a 3rd party supplier, Forcepoint. When this service was procured WBC considered the statutory guidance and believe the solution provides 'appropriate web filtering'.

The technology uses a category system to define what type of content each website represents, such as education, business, drugs, malware etc. That category determines whether a school can or cannot access that specific site.

Forcepoint have an Advanced Classification Engine that performs in depth, real-time inspection of content to categorise web sites and protect users from accessing inappropriate content and malware.

Each School has categories deemed potentially harmful and/or inappropriate blocked by default and then can have rules to block or allow certain sites as per their individual requirements.

The service, transparent to the end user, intercepts internet traffic from across the School's Network(s) and is designed to protect staff and learners as much as possible.

Forcepoint have provided a response to the UK Safer Internet Centre's Monitoring Checklist, it can be viewed here.

All internet traffic that passes through the WBC internet connection will be filtered and there is no requirement for specific configuration on the hardware (PCs, laptops, Ipads, Chromebooks etc...).

Industry Standards

The **UK Safer Internet Centre** States the following: (Link)

> "Recognising that no filter can guarantee to be 100% effective, schools should be satisfied that their filtering system manages the following content (and web search):
>
> - Discrimination – Promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010
> - Drugs / Substance abuse – displays or promotes the illegal use of drugs or substances
> - Extremism – promotes terrorism and terrorist ideologies, violence or intolerance
> - Malware / Hacking – promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
> - Pornography – displays sexual acts or explicit images
> - Piracy and copyright theft – includes illegal provision of copyrighted material
> - Self-Harm – promotes or displays deliberate self-harm (including suicide and eating disorders)
> - Violence – displays or promotes the use of physical force intended to hurt or kill"

If a School does find a website that they feel is inappropriate it should be reported to the Council's IT team for investigation, WBC are able to block websites as the need arises and inform Forcepoint so they can take the appropriate categorisation action.

The internet currently contains in excess of 1 billion sites, with an estimate of 250,000 new websites appearing every day. Occasionally things can slip through and be categorised incorrectly. This will occur for any provider offering filtering services. In our experience this does not happen often for Schools with the WBC Network Service.

It would be a danger to allow access to sites that have not yet ben categorised. As a default setting, WBC block any 'uncategorised' sites to minimise this risk.

If a School attempts to access a new site or one that is not known to the database they will find that access is denied. For genuine websites they can log a call with WBC IT and the site will then be categorised appropriately and access will be allowed.

Guidance: Filtering Exceptions & SafeSearch

Exceptions

There are some circumstances where a filtering system does not appear to take any effect, these are:

- Google images
- You tube, or similar video sharing platforms
- Other websites that collect and display clipart and/or images
- Website adverts

Schools have occasionally reported that when using Google images it has brought back an image that was considered inappropriate. This is because:

- WBC allow access to Google as a website.
- Google is actually a search engine and searches the internet, creating links to any sites and/or media found regardless of actual content.
- So when you search in Google you can receive a very wide response from seemingly innocent search words.

SafeSearch

The search function within Google does have something called “SafeSearch” and this is enforced by default.

Google’s statement around the “SafeSearch” service is as follows

> *“You can filter explicit search results on Google, like pornography, with the SafeSearch setting. SafeSearch isn’t 100% accurate. But it can help you avoid explicit and inappropriate search results on your phone, tablet, or computer.”*

Google then go onto state:

> *“We do our best to keep the SafeSearch filter as thorough as possible, but sometimes explicit content, like porn or nudity, makes it through. If you have SafeSearch turned on, but still see inappropriate sites or images, let us know.”*

They then provide instructions on how to report inappropriate content to them. Google also provide additional disclaimers about content that may be accessible via their website.

The Council’s web filtering system allows access to Google and to Google images, but does not filter the images or content viewed directly within the site, as this is controlled directly by Google.

Google also own You Tube and offer similar advice relating to videos. As with Google images, the Council’s web filtering service controls if you can or cannot access You Tube. SafeSearch is enabled by default, but occasionally inappropriate videos can appear.

Outside of Google images, there are other websites that can collect clipart from the internet and display it for you. These sites are potentially higher risk as they do not operate under the Google SafeSearch option and provide little to no way of reporting back inappropriate content.

Advertising

Many websites carry adverts for other websites. Sometimes the adverts are trying to sell you something. Just as often they are "clickbait" and if you click on the link the content you see isn't related to the advert.

These adverts may use inappropriate imagery in order to attract people to click on the link. The web filter is unable to block these adverts. The only action WBC could take for schools is to block the website showing the advert but in practice this is not proportional. So many sites contain adverts you could end up blocking half of the internet.

The blocking in itself may be in itself inappropriate as the guidelines warn against over blocking.

A statement from the Safer Internet Centre says:

> *"Schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."."*

Guidance: Monitoring and Reporting

The **UK Safer Internet Centre** States the following: (Link)

"There are a range of monitoring strategies and systems however the appropriate monitoring strategy selected should be informed by your risk assessment and circumstances. It is also vitally important to also review and refine the relevant policies as part of assessing (or implementing) a monitoring strategy or system. The following are examples.

1) Physical Monitoring

Physical monitoring can contribute where circumstances and the assessment suggests low risk, with staff directly supervising children on a one to one ratio whilst using technology. This could be: physical supervision of children whilst using the Internet; assigning additional classroom support staff to monitor screen activity; or actively monitoring all screen activity during a lesson from a central console using appropriate technology.

2) Internet and web access

Some Internet Service Providers or filtering providers provide log file information that details and attributes websites access and search term usage against individuals. Through regular monitoring, this information could enable schools to identify and intervene with issues concerning access or searches.

3) Active/Pro-active technology monitoring services

Where the risk is assessed as higher, Active or Pro-active monitoring technologies may be suitable. These specialist services provide technology based monitoring systems that actively monitor use through keywords and other indicators across devices. These can prove particularly effective in drawing attention to concerning behaviours, communications or access."

Currently Monitoring and Reporting is not included as standard as part of the Network Service, although log file reports can be provided if requested. The caveat with these reports is that they take time to produce and, if your School does not have the system configured with your Curriculum Active Directory it will display information that makes it hard to identify who accessed the inappropriate content, it will look at the IP address of the device and this will help identify the device that was used but not necessarily who was logged into it at that time.

If the School assesses the risks and you believe that the Monitoring and Reporting provided by WBC does not meet your individual requirements and policy/strategy there are some options available:

- WBC review and change service. If a significant number of Schools request this we are happy to look at the options, up to now there has not been enough Schools requesting this.
- School procures their own solution. Some Schools have procured and implemented their own web filtering service and had it installed on their School Network(s).

Please be aware when looking at any alternative options that there are some considerations that Schools need to be aware of:

- Cost vs Benefit – as you would expect, the more functionality a system offers the more it is likely to cost. The School should consider whether the benefits gained mean value for money.
- Configuration – to take advantage of some systems monitoring and reporting it requires extra configuration from the School's IT provider(s) and this should be taken into account when costing up a service, i.e. to monitor who is accessing something you may need to have logins set up for each individual pupil and have this linked to the system.
- Training / staff responsibilities – having a system that reports on inappropriate internet activity or alerts the school at the time when something is being accessed (real-time monitoring and alerts) will require staff at the school to be trained in how to use the system and deal with any alerts, also these staff members would need time to carry out these tasks.

Recommendations for Schools

WBC have taken the necessary steps to procure, provide and support a web filtering solution appropriate for Schools. However, each School also has responsibilities to ensure their Networks and IT provisions are as safe as possible.

The following are WBC's recommendations for schools:

- School leaders should regularly review which websites (like You Tube, etc.) the School wishes to be blocked by default and inform WBC so that the correct policies can be applied to the School.

- If a School user finds a website they feel is inappropriate, report it to WBC.

- If the School's IT Network / Curriculum Network is supported by another supplier / member of School staff then the School should ensure they implement the advised proxy and DNS settings. This will ensure Google SafeSearch is enabled across the School.
  - Proxy – We no longer operate a proxy service and so NO proxy settings are required to access the Internet on the Curriculum Network.

- DNS – To ensure Google SafeSearch is enabled you must use the following DNS servers: Primary Setting - 5.61.120.6 and Secondary Setting - 5.61.120.10.
  Please ensure no other DNS settings are present (including Google settings) as this has the potential to override the WBC settings and compromise SafeSearch for the School.

- The School should have robust policies in place for dealing with any instances where a user accesses inappropriate material.

- Schools should ensure staff are aware of how the web filtering service works.

- Teaching staff should exercise care when planning lessons that use the internet. Appropriate levels of supervision should be exercised.

Considerations for Schools

For all of the reasons mentioned, this is a complex area to understand and make decisions about. This is compounded because:

- The legislation is constantly evolving
- The legislation is open to some interpretation and schools are left to a large part to try and determine what this means to them
- There is the influence of external providers who in some cases are trying to get to schools to buy things they don't necessarily need in order to profit financially

To help you navigate this:

- We believe the service offered by the Council meets the requirements of the current legislation for appropriate filtering as defined earlier in this document
- As and when the legislation changes in the future, we will review our offering and amend it accordingly. Changes to service prices may or may be not needed depending on how the requirements change.

Some schools have stated their interest in more advanced service options such as increased reporting frequency, activity by user, age differentiation, real-time reporting, etc.

It is ultimately the decision of the school as to how critical they feel these requirements, what the benefits are and how proportionate these are to the costs involved.

The information provided in this document is aimed to support Schools in understanding the service in place and assist with assessing the options going forward.