

**Please note that the filtering statement only applies to Schools meeting the following criteria**

- School has signed up to the full network service as offered by WBC ICT
- School has followed the guidance offered from WBC ICT and changed Primary and Secondary DNS entries to recommended settings, the use of any other DNS entries will invalidate this statement
- School understands that this statement does not apply to mobile 3G/4G networks
- The school has a robust online safety policy

**What is the Web Filtering service?**

The schools' web filtering service provides a filter for staff and learners preventing them from accessing potentially harmful online content. The service, transparent to the end user, intercepts all internet traffic from the school's curriculum network which connects via the WBC broadband circuit (WAN) provided as part of the Network SLA.

Web filtering is configured using various policies. These policies can be set globally for all schools or at an individual level depending on the specific requirements requested by the school which may include:

- Time of day
- Time of week for specific clubs or groups
- Website specific e.g. Facebook

Individual schools can request greater control for their school in line with individual school policies and the Keeping Children Safe in Education (KCSIE) guidance 2016.

Endpoints (PCs, laptops, iPads) on the curriculum network do not need any specific configuration for the web filtering to be applied, ensuring all web bound traffic from the school's curriculum network is filtered. However your 3<sup>rd</sup> party may need to change some configuration on the curriculum network in order to ensure Google and Bing search.

The following disclaimer is published by the UK Safer Internet Centre:

**"It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision"**

In the event of a site being discovered that is deemed inappropriate by the school, this should be logged via 2200, so the WBC ICT team can investigate and take appropriate action. This will be done within the existing service SLA.

**How does web filtering work?**

Web filtering blocks access to potentially harmful online material from staff and learners by categorising online content e.g. pornography, gaming, gambling, social media, etc.

**Statement from our provider – Fortinet:**

"General categorisation is based on an automated categorisation engine which has been developed in-house and which has evolved over more than 13 years since its initial conception. The system uses language dictionaries to allow support in any language. Sites are scanned based on a number of methods:

- new pages on identified popular sites
- URLs which are requested by a user, but which are not rated. Such URLs will go into a queue to be rated based on hit count and the current charge on the system.
- Bulk requests from a specific customer. Such requests are treated case by case, but we generally offer this as a free service.

- Individual requests received from customers or users. These requests can be received in a number of ways (see below) and may be either requests to rate an unrated site, or requests to change the rating of a site.

In general, initial rating is done by the automated rating system. Malicious content (viruses, exploits) is not rated using this system (more details below) because such sites generally have legitimate visible content. Ratings may also be obtained from third-party feeds, including feeds from governments or other organisations, containing such content as extremism or sexual violence. Requests to change the rating of an already categorised URL will always be dealt with by a human, to ensure that the request gets the highest level of care and attention.

- A flexible hierarchical search system is used which allows ratings to be given to anything from a top-level domain or an IP address, right down to a fully-specified URL. This allows for example a blogging site such as wordpress.com to have a "Personal Websites and Blogs" rating, whilst individual blogs can have a rating based on their actual content. It also ensures that the entire wordpress domain is not blocked just because a single blogger posts inappropriate content. "

### ***Does the service provide appropriate filtering and monitoring?***

From September 2016, the DfE revised their statutory guidance "Keeping Children Safe in Education" with specific reference to web filtering. The following requirement has now been added:

*"Schools are obligated to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" however, 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."*

The UK Safer internet centre, has published provider checklists around appropriate filtering and appropriate monitoring:

<http://www.saferinternet.org.uk/advice-centre/teachers-and-professionals/appropriate-filtering-and-monitoring>,

To ensure the service we provide to schools meets these criteria, we have asked our supplier Fortinet to complete these checklists which will act as a baseline statement of assurance around the appropriate filtering and appropriate monitoring service.

**From the information provided to us by our supplier Fortinet thus far, WBC ICT department believe that the web filtering solution as configured meets the current DfE guidance.**

The responses from Fortinet can be found here for filtering:

[Appropriate Filtering Fortinet Response](#)

And here for monitoring:

[Appropriate Monitoring Fortinet Response](#)