Wave9
Managed Services Limited

WaveConnect Internet Services for Schools

Supporting Security, Safeguarding and Prevent

Version Number	1.1
Status	Final
Date	15.1.16

Table of Contents

Stay Safe – Security, Safeguarding & Prevent

1. Overview

We're here to help school leadership and IT teams choose and implement the right IT solutions that will meet their changing needs and help them comply with government legislation and guidelines for keeping children safe.

Whilst we all know e-safety is about education, rather than "lock down" of systems, it is important that education appropriate services are procured by schools and that they can demonstrate, when asked, how their infrastructure and systems support their e-safety policies and procedures.

Our WaveConnect Internet Service is specifically designed for schools and demonstrates a comprehensive approach to security and filtering.

2. What is being asked of Schools?

2.1. Keeping Children Safe in Education

In December 2015, the Department for Education published proposed changes to 'Keeping Children Safe in Education' for consultation applying to schools in England.

Amongst the proposed changes, schools will be 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."*

2.2. Prevent

Schools in England and Wales are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, 2015).

Furthermore, it expects that they *"assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology".* There are a number of self-review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

The WaveConnect Internet Service for Education helps you meet these overarching requirements and goes much further to support guidelines around enhanced usage monitoring and reporting.

Read on and we'll explain how…..

3. The WaveConnect Internet Service for Education

WaveConnect is designed and operated in partnership with Sophos. Sophos is a market leader in IT security and has been helping UK Education establishments to protect students and staff against malicious software, inappropriate content and other threats, for many years.

Sophos security and data protection protect 6 million administrators, teachers, and students around the world.

3.1. WaveConnect & Sophos Labs

Each WaveConnect appliance is connected to SophosLabs

SophosLabs collect, correlate and analyse data to provide the best protection for every Sophos customer. Sophos have developed a state of the art analytics system so they can efficiently process the millions of emails, URLs, files, and other data points that come into the labs each day.

Sophos draw upon this data and extensive experience to keep both their anti virus (AV) engine and web filter database, containing 35 million+ sites in 96 categories, ahead of emerging internet threats.

Using facilities in Australia, Hungary, England, and Canada they “follow the sun” ensuring analysts are on duty to respond to new threats and analyse customer submissions 24/7/365.

Unlike competing solutions that rely on third parties, Sophos develops its URL filtering databases and AV engines in house. This ensures our customers are always the first to be protected against the latest threats and inappropriate websites.

3.2. WaveConnect and the Internet Watch Foundation (IWF)

A partnership with the Internet Watch Foundation ensures maintenance of a list of known illegal, inappropriate and criminal sites to block. It also helps ensures that WaveConnect education customers meet the recommendations of the Government’s “Prevent” directive.

When the Internet Watch Foundation update their lists of websites, Sophos add these to the web filtering database and push updates immediately to the WaveConnect appliance in school. This ensures there is no window of vulnerability where a child could be exposed to illegal, inappropriate or radicalisation content while waiting for a scheduled maintenance update.

Other solutions that depend on third parties to supply and maintain their AV and web filter database don’t have this capability to apply immediate updates. Schools using these products, potentially expose students to unsuitable content during the period before the update is released and applied.

3.3. WaveConnect and the CTIRU (Counter Terrorism Internet Referral Unit)

The Criminal Activity category is one of 96 different web categories available for selection within the Web Filter and is applied in schools filtering policy by default. It is key to supporting Prevent.

The category includes data supplied by the CTIRU. Such as;

- speeches or essays calling for racial or religious violence
- videos of violence with messages of ‘glorification’ or praise for the attackers,
- chat forums with postings calling for people to commit acts of terrorism or violent extremism,
- messages intended to stir up hatred against any religious or ethnic group
- bomb-making instructions.

We also include Violence, Discrimination and Extreme categories to further filter out radicalisation sites to ensure children are safe from terrorist and extremist material.

3.4. WaveConnect and YouTube for Schools

WaveConnect is optimised for integration with YouTube for Schools which allows schools to limit YouTube access to educational-approved content along with any videos specifically approved by the administrator (YouTube for schools is changing in July 2016 - more information on this program and how you can access it is available at youtube.com).

3.5. WaveConnect and Application Control

Social Media has become a key channel used for cyber bullying and by criminals for the radicalisation of students. WaveConnect allows you to control and limit the use of applications such as Facebook, Bittorrent and Skype. Applications can be blocked or access can be limited by profile.

This allows you the flexibility to structure different policies for children across key stages for example. Additionally, you can also enforce the safe-search features of Google, Yahoo and Bing.

3.6. WaveConnect and Endpoint Protection (Optional)

With endpoint protection, you get complete web protection everywhere for your pupils —in class, at home, or on the school bus. For endpoint customers, our appliance works seamlessly with your Secured Windows Endpoints to provide complete web protection for offsite users. When they leave the local network, Endpoint protection takes over, providing full enforcement and protection everywhere they go. Policy updates and browsing activity are automatically synchronised.

Staff and students are protected from radicalisation content even when working remotely, and your IT team doesn't have to rely on directing web traffic back to the school which can slow internet access down.

4. Meeting the Requirement: Appropriate Filtering and Monitoring

It is important to distinguish between "filtering" and "monitoring".

Filtering services are usually provided by your Internet Service Provider as part of your broadband package, they protect children and staff from accidentally encountering or intentionally accessing inappropriate sites and content, such as pornography, vulgar language, and hate sites.

Monitoring Tools (e.g. Impero) may be deployed to highlight when a pupil types a word, phrase or acronym that may suggest cyberbullying, inappropriate behavior or those at potential risk for things like eating disorders, self-harm, suicide and violence. These are additional 3rd part applications that can supplement your e-safety systems in school.

The following section provides an overview of how WaveConnect meets the *Filtering* criteria for Schools Internet Services and can support *Monitoring* as defined by the UK safer Internet Centre.

4.1. Appropriate Filtering

Area	Requirement	Meets Requirement?
Illegal Online Content	Are IWF members and block access to illegal Child Abuse Images and Content (CAIC)	Yes – See 3.2
	Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	Yes – See 3.3
Inappropriate Online Content	Filtering manages the following Content • Discrimination • Drugs and substance abuse • Extremism • Malware/Hacking • Pornography • Piracy and Copyright theft • Self Harm • Violence	Yes – see 3.1
Recommended System Features	**Age appropriate, differentiated filtering** – includes the ability to vary filtering strength appropriate to age and role	Yes via AD
	Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content	Yes via Web Console
	Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	Yes 96 separate categories with school decision to block / allow
	Identification - the filtering system should have the ability to identify users	Yes - via single sign on and/or ip address
	Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies	Layer 7 application control can be applied
	Network level - filtering should be applied at 'network level' i.e., not reliant on any software on user devices	Yes – no client software required
	Reporting mechanism – the ability to report inappropriate content for access or blocking	A range of standard and customisable reports can be viewed or automated
	Reports – the system offers clear historical information on the websites visited by your users	Logfiles are kept – capability for 12 months plus for and average secondary school

4.2. Appropriate Monitoring

Usage monitoring can be demonstrated in 3 main ways. Your risk assessment and understanding of your school will inform your practice and what approach you take.

4.2.1. Physical Monitoring

Most suited where circumstances and the assessment suggests low risk, with staff directly supervising children 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.

The following are possible limitations or points to consider

- Can be resource intensive
- Less effective across a larger group or a group using mobile devices
- Students often adapt screen behaviour to avoid monitoring

An advantage could be immediate intervention when an issue arises, which can be developed as a teaching opportunity

4.2.2. Internet and Web Access

Unlike some providers, on request WaveConnect is able to provide logfile information that details and attributes websites access and search term usage against individuals. This can be set to send on a regular basis to a designated member of staff. Through regular monitoring, this information enables schools to identify and intervene with issues concerning access or searches.

Bear in mind

- Logs need to be regularly reviewed, interpreted and alerts prioritised for intervention
- Information held by the school that indicates potential harm, must be acted upon
- Be aware of any limitations of the logfile information or interpretation thereof

4.2.3. 3rd Party Monitoring Services

Where the risk is assessed as higher, Active or Pro-active monitoring technologies may be suitable. (E.G Policy Central / Impero)

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.

These systems can take the form of:

- Active monitoring where a system generates alerts for the school to act upon
- Pro-active monitoring where alerts are managed by a third-party provider and may offer support with intervention.

The following are possible limitations or points to consider

- Can be expensive in terms of installing and maintaining technology
- Pro-active monitoring uses specialist organisations and may involve additional expense

- Active monitoring requires sufficient internal capability and capacity
- Active monitoring can initially generate significant volumes of information and alerts which can be difficult to interrogate and interpret.

5. Summary

In choosing WaveConnect for your school internet requirements you will benefit from a service that incorporate some of the best Security and Safeguarding technology available today.

Our partner Sophos is a market leader in Unified Threat Management (UTM) Technology and education is a key sector to which they apply significant resource and expertise.

Whilst school ICT systems play their part in keeping children safe, education is paramount. Promoting e-safety and embedding it in to the curriculum, so children become safe and responsible users of technology has a long lasting impact.

Should you require further information about WaveConnect or how your school may develop it's e-safety practice then please do get in touch.