Appropriate Filtering for Education settings

June 2017

Provider Checklist Reponses

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" . Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England 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."

Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to "have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined 'appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

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.

Company / Organisation	eSafety4schools
Address	Unit 4, Cotswold Business Park, Caddington, Bedfordshire, LU1 4AJ
Contact details	matthew@esafety4schools.com
Filtering System	Managed iboss deployed from our Datacentres
Date of assessment	19/2/2018

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

.

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
• Are IWF members		iboss has been a Member since 2013
• and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		The IWF CAIC list is updated upon receipt and is in a restricted Category.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		This list is integrated and updated upon receipt.

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		The iboss product places Discrimination content into **Violence and Hate** category – which is blocked by default as part of our service
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		The iboss product places Drugs/Substance abuse content into the **Drugs** category – which is blocked by default as part of our service
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		The iboss product places Extremism content into the **Violence and Hate** category – which is blocked by default as part of our service
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		The iboss product places Malware/Hacking content into the **Malware** category - which is blocked by default as part of our service
Pornography	displays sexual acts or explicit images		The iboss product places Pornography and Pornographic content into the **Porn** category - which is blocked by default as part of our service
Piracy and	includes illegal provision of		

copyright theft	copyrighted material		The iboss product places Piracy and copyright theft content into the **File Sharing** category - which is blocked by default as part of our service
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		The iboss product places Self Harm content into the **Violence and Hate** category – which is blocked by default as part of our service
Violence	Displays or promotes the use of physical force intended to hurt or kill		The iboss product places Violence content into the **Violence and Hate** category – which is blocked by default as part of our service

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

Application (Layer 7), controls such as Games, Chat, IM, P2P, command line tools, etc.
Layered Google service controls (Safe Search, Safe image Search, Youtube and Gmail controls)
Deep Packet Inspection (DPI), for evasive applications such as Tor, BitTorrent, Ultrasurf, Psiphon etc.
Browser and OS controls
File extension and MIME type download controls.
Social Media Controls (Facebook, Twitter, Pinterest etc)
Port Blocking
Sleep Schedules
Keyword's with high risk real-time alerting
Real-time monitoring

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

All categories have 3 modes**, Allow, Block and Stealth**.
Stealth mode can be used for content monitoring without blocking content.
All categories also have priorities so that categories can be weighted appropriately for the policy type or age rating. For example, if the games category is priority 0 and blocked, and the education category is priority 1 and allowed – game web sites with no education content will only be placed into the games category and therefore blocked. However, game web sites with educational game content will be placed into both the games and education category, and as the education category has a higher priority and is allowed, the educational game web sites will be allowed.
Policy groups can also have an 'Overide' option set which allows teaching staff to override blocked content without intervention from the web filter administrator by entering their credentials into a block page. This feature is time based to ensure that the page returns to its previous categorisation once the over-ride period is over.
Block pages can have 'exceptions per policy'. This allows for feedback to be sent to the filtering

administrator, directly from the block page, including a reason why the web site should be unblocked. Exceptions can generate real-time alerts and have their own administration area for easy unblock/block tasks – this is also a service eSafety4schools undertakes on behalf of schools should they have opted for the full Managed Filtering option.
Alternatively either the schools network manager or their 3rd part support company can be provided with the credentials to undertake this task
Uncategorized URL's can be blocked, blocked with override controls and are per policy.

Filtering System Features

How does the filtering system meet the following principles:

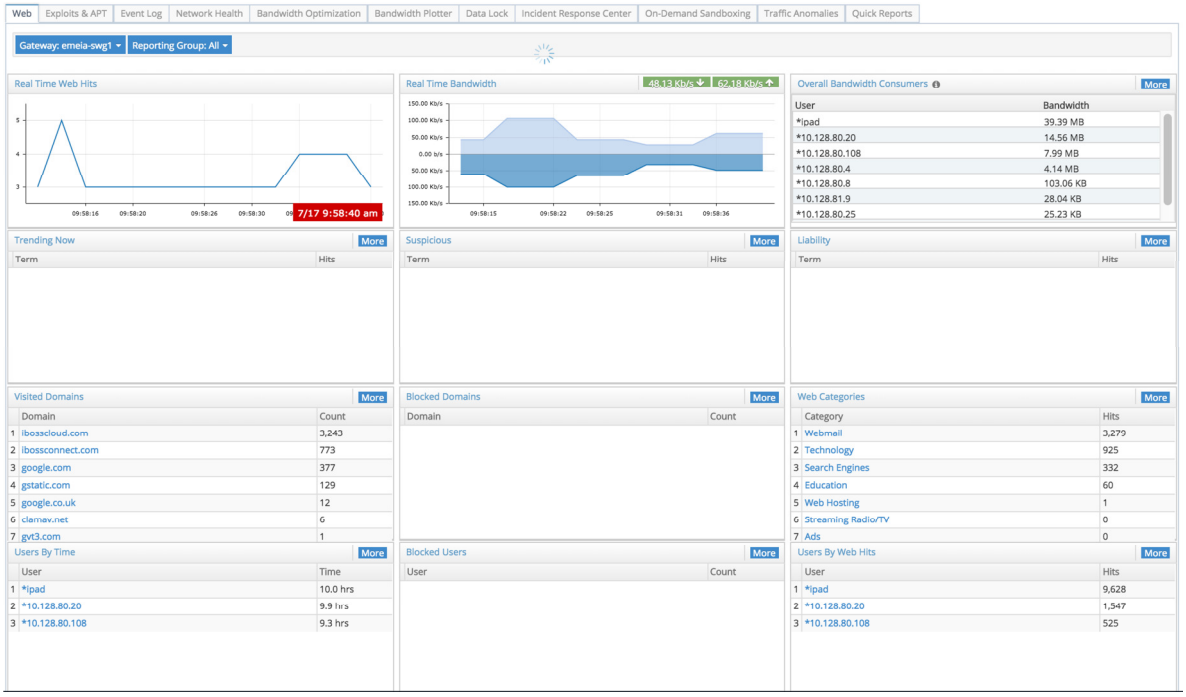
Principle	Rating	Explanation
• Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		eSafety4schools deploys iboss to schools as requested by schools so this can be Polices based on MS AD groups, or per year group. Each group of users can have a number of polices applied to them based on time e.g. stricter in the day, more relaxed at lunch time/evening and categories can be weighted to allow further granularity.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		Prior to provisioning the Web Filtering service eSafety4schools requests information from the school regarding whom they should set up as administrators – as it can be staff within the school, an approved 3rd party IT support company or an LA support technician. On set up the school is sent a Welcome Letter confirming each requested users log on credentials for access to the Web Filtering platform. An easy to follow user guide is also sent to ensure that all approved administrators can manage the schools web filtering –by amending or updating polices and rules and generating Internet usage reports. A standard feature of the iboss product is to allow a teacher over-ride option – whereby a user logged in as a teacher can just hit a link on the deny page to allow access to the denied site. Usage of the over-ride option is recorded and reported on and the action only has a fixed time span i.e. the page reverts to its normal status once the over-ride 'time' has expired, thus the site returns to its denied status on that machine.

		This feature ensure that a teacher can continue to teach even if they are trying to access a denied site – without needing to ask for technical assistance or be delayed waiting for the designated person to allow access to a site. To note not all categories allow the over-ride features – those that should be blocked at all times Porn/Drugs etc., remain blocked even when this feature is enabled.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		eSafety4schools prides itself on its close working relationship with both its school's customers and its vendor partner iboss. As such whilst we defer to the iboss classification and categorisation as a norm we are perfectly able and willing to make bespoke alteration to the platform should it be required. As well as iboss we also partner with a couple of Monitoring vendors and on occasion their software will pick up sites that have sneaked through the filtering, at such times we can over-ride the iboss categorisation and either block or allow the site – whichever is the appropriate action. Additionally, as a service company we run daily reports across our entire deployed estate of schools (some 500) to see which sites are the most popular and ensure As a global company iboss provides it filtering and malware defence solutions with highly configurable controls so as to meet the various governance and compliance regulations in different countries. The classification policy can be found here: http://resources.iboss.com/product/help/ibe/en_US/v2/webfilter_help.html
● Identification - the filtering system should have the ability to identify		The iboss SWG can integrate with multiple directory and SSO environments including

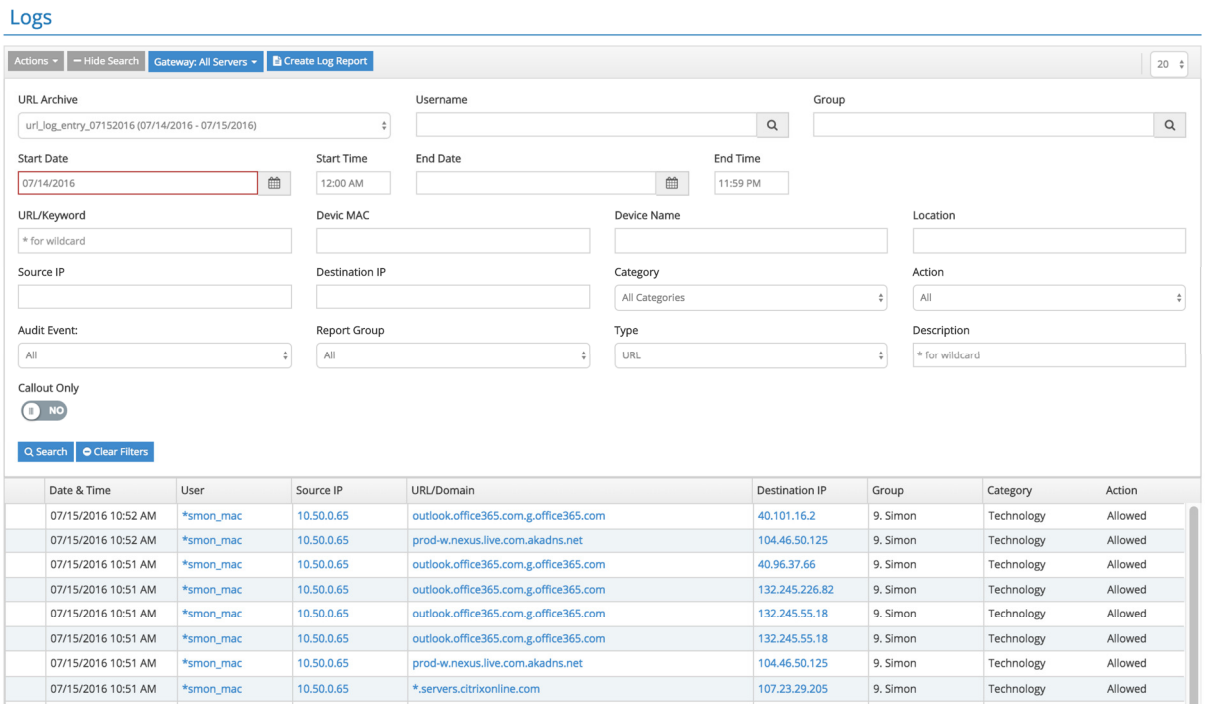
users		Active Directory, SAML, Radius (802.1x, Wireless, NAC), E-directory, OpenDirectory, LDAP, Google SSO, and has options for BYOD and 'non-domain' joined devices (iOS). eSafety4schools as part of the service will work with the school to determine the preferred identification methodology and during the provisioning process deploy as agreed thus all schools need to do is keep the main directory up to date to ensure they have per user filtering and reporting at all times.
• Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)		As a full Secure Web Gateway (SWG) product rather than just an http/https filtering product iboss inspects all web streams (all TCP and UDP ports), and has full visibility of bi-directional web traffic from any type of web application not just web browsers. This allows the SWG to have granular controls for mobile, guest and BYOD devices including non-browser based applications.
● Multiple language support – the ability for the system to manage relevant languages		As an International company iboss has the ability to categorise content in any language and logging and keyword controls accept any character set (Unicode).
● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		eSafety4schools has built a fully redundant cloud based Web Filtering service based on the iboss SWG product. The service is delivered from the cloud or for larger secondary's/MAT's we can build a hybrid deployment where large sites have servers but smaller sites are pure cloud – all linked into a single management interface. No client deployment is required at all; however we also offer a managed PREVENT monitoring service that does require a client on each device, this is a separate service for which a separate response has been made
● Reporting mechanism – the ability to report inappropriate content for access or blocking		The iboss SWG has an inbuilt micro SIEM known as the 'Reporting and Analytics console'. Which eSafety4schools delivers to each of its schools from the cloud to provide real-time reporting (pic1), and

		monitoring, query reports (pic2), drill down reports(pic3), and scheduled reports. In addition, real-time alerting and desktop video recording can be triggered on keywords, attempted access to blocked categories, or use of evasive or high risk applications (plus device quarantine)
• Reports – the system offers clear historical information on the websites visited by your users		eSafety4schools manages the URL and Event logging via its cloud based iboss 'Reporting and Analytics' console. This includes granular historical reporting that is customizable and exportable into popular formats (HTML, CSV, PDF etc). Reporting to external systems such as SIEM's is also supported via API or Syslog.

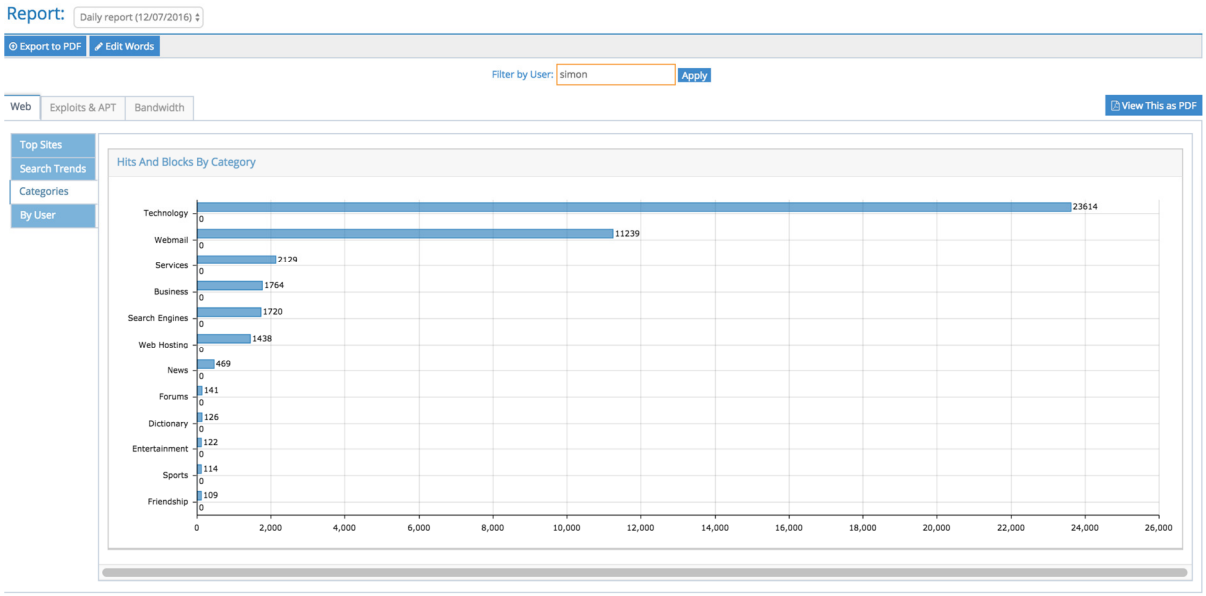
Pic 1 – Real-time Report / Monitoring



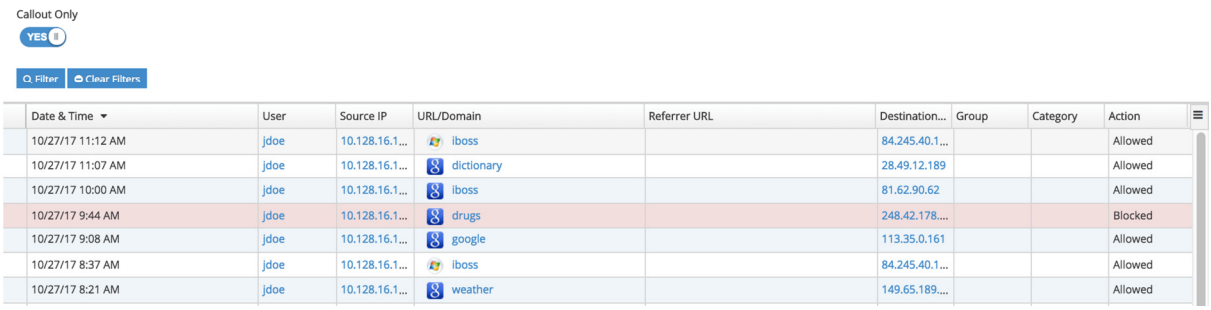
Pic 2 - Query report example.

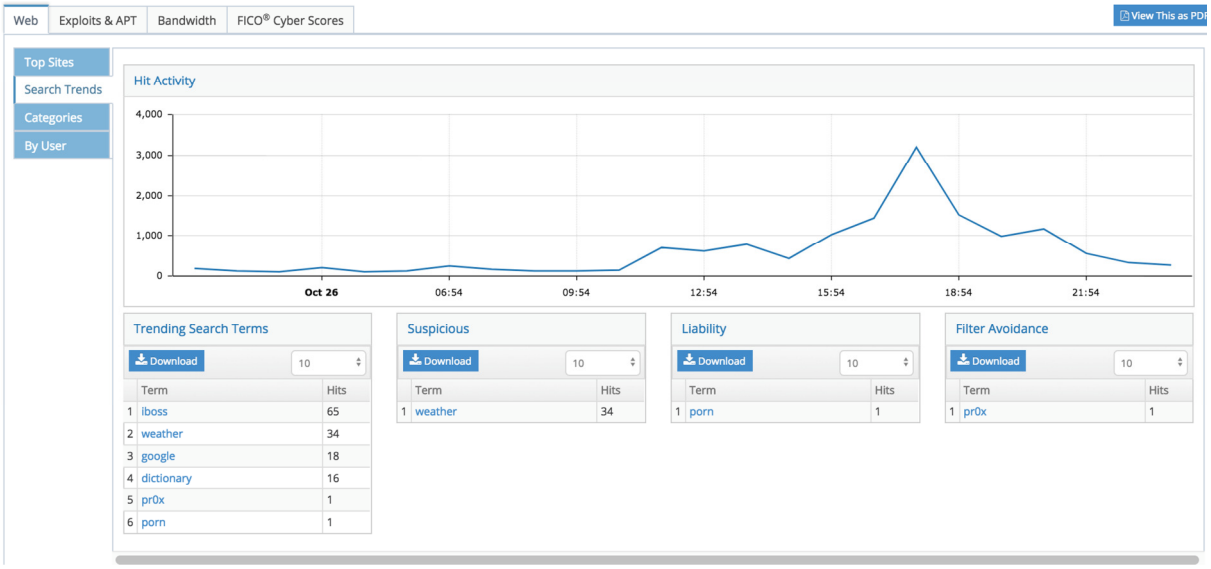


Pic 3 – Drill down reports



Search Query reporting





Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum*".[1]

Please note below opportunities to support schools (and other settings) in this regard

In April 2018 eSafety4schools will be introducing Monthly Safeguarding blogs to assists schools.

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Matthew Holt
Position	Director
Date	19/02/2018
Signature	M. Holt