Appropriate Filtering for Education settings

June 2018

Filtering 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	
Address	
Contact details	
Filtering System	
Date of assessment	

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		Member since 2013
• and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		Yes - CAIC list 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 can be locked.

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.		Placed into violence and hate category
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Placed into Drugs category
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Placed into violence and hate, and/or Terrorism / Radicalization Category
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Placed into Malware and Hacking categories
Pornography	displays sexual acts or explicit images		Placed into Porn Category
Piracy and copyright theft	includes illegal provision of copyrighted material		Placed into Piracy category
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Placed into Violence and Hate category
Violence	Displays or promotes the use of physical force intended to hurt or kill		Placed into Violence and Hate category

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 a 'Overide' option set which allows staff or students to override blocked content without intervention from the web filter administrator.
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.
Uncategorized URL's can be blocked, blocked with override controls and are per policy.

Filtering System Features

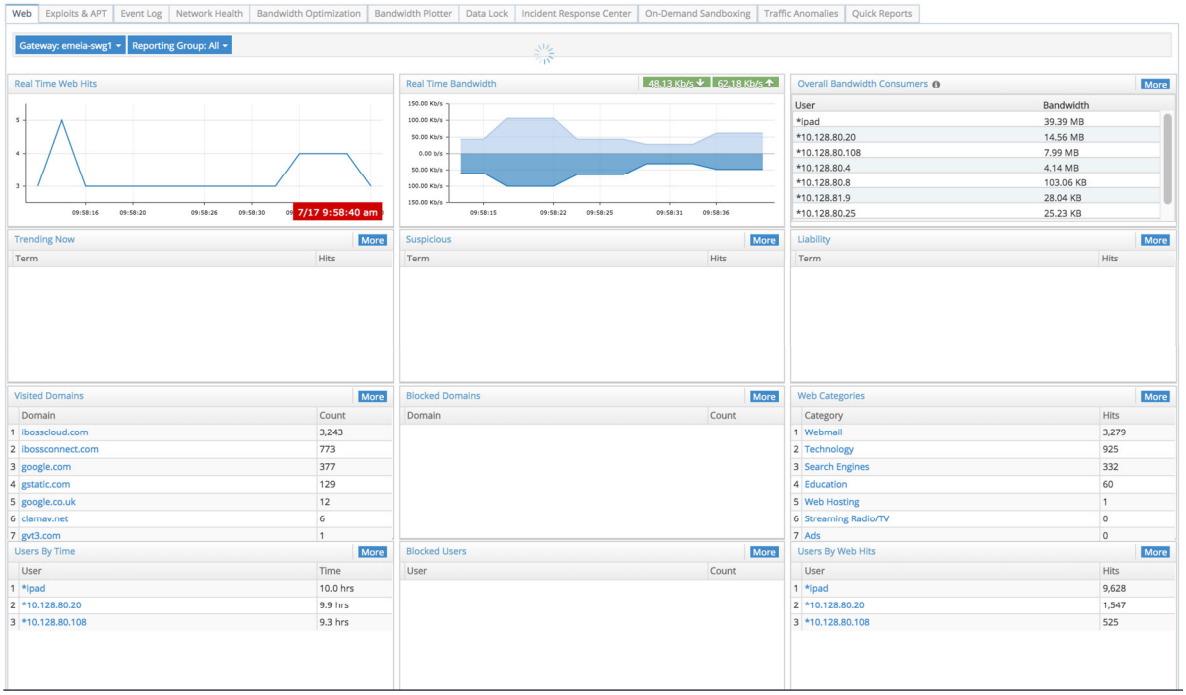
How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		Policies can be per year, group, or classroom with weighted categories.
• Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services		Full analysis of all TCP and UDP ports with algorithms to detect, block and quarantine endpoints running evasive applications such as: • Tor • Psiphon • Ultrasurf • OpenVPN • BitTorrents • Chat Apps • + Others
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		All controls are intuitive with context sensitive online help and can provide delegated

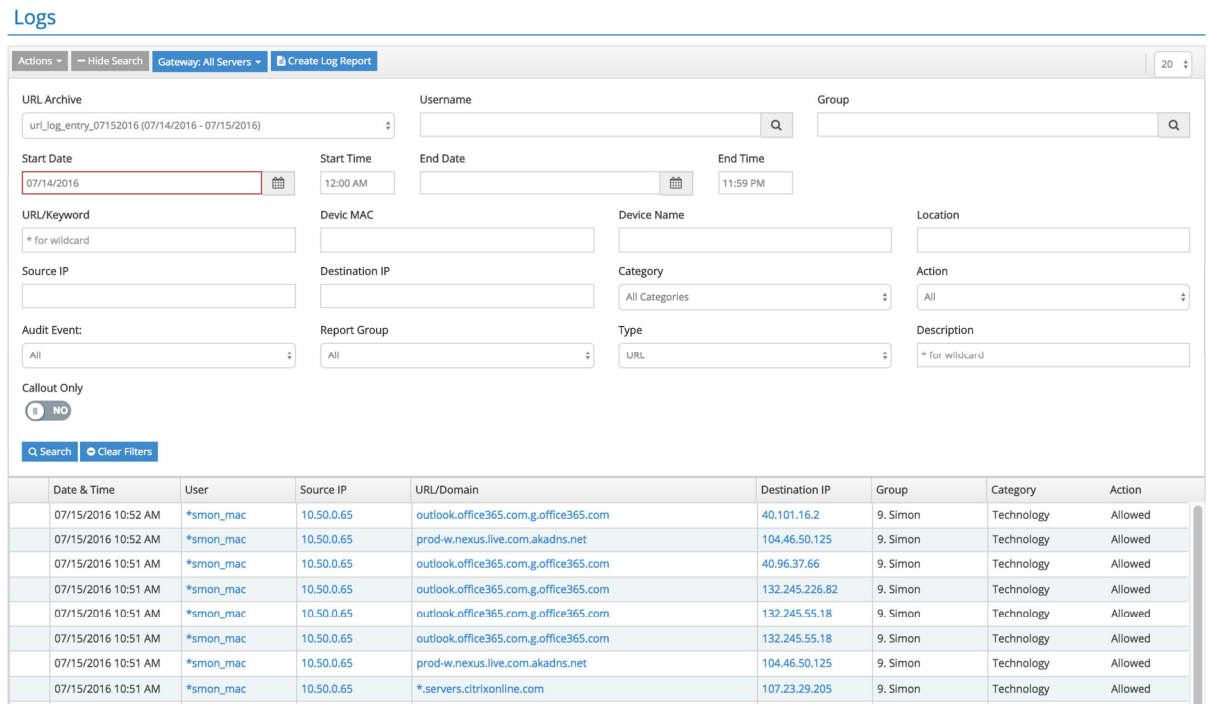
		access to teaching staff. All controls are via a reactive web console that fits to any screen size.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		As a global company iboss provides 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: https://support.ibosscloud.com/hc/en-us/articles/115008039947-Web-Category-Descriptions
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		The iboss cloud management platform provides a 'Single Pane of Glass' management view. The node based architecture of the iboss Distributed Gateway Platform allows filtering gateways to be located anywhere and then cloud joined for centralized management and reporting. The role based and delegated administration model of the platform means that multiple administrators can manage the gateways, and ISP's or MSP's can manage multiple environments and accounts from a single console.
• Identification - the filtering system should have the ability to identify users		The iboss SWG integrates with multiple directory and SSO environments including but limited to: 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).
• 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 iboss SWG inspects all web streams (all TCP and UDP ports), and has full visibility of bi-directional

the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)		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		Content can be categorized 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		The iboss SWG is a gateway device and does not require endpoint software to be deployed. The SWG can be deployed on-premise in-band, out-of-band, or in the cloud (includes hybrid)
● 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'. This separated reporting console has 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		URL and Event logging is via the iboss 'Reporting and Analytics' console that 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.

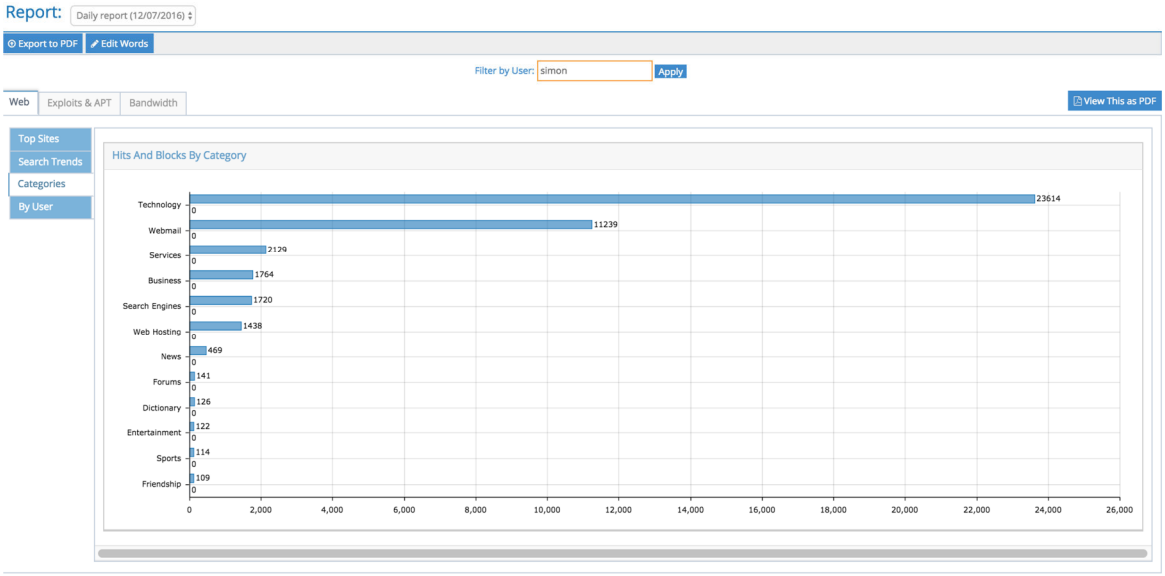
Pic 1 – Real-time Report / Monitoring



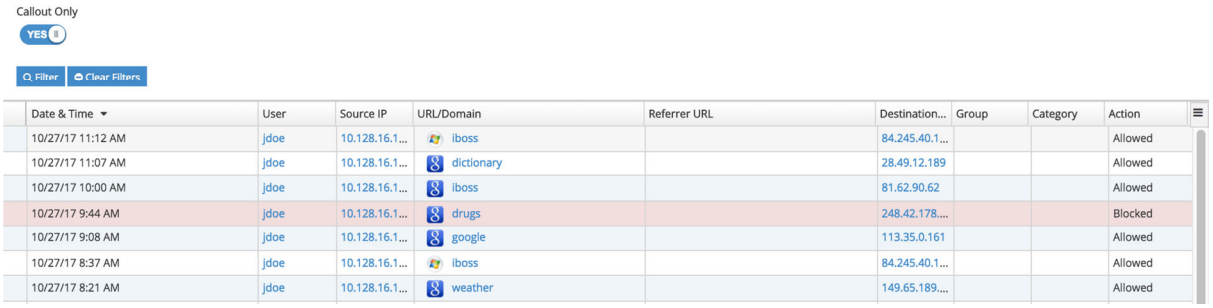
Pic 2 - Query report example.



Pic 3 – Drill down reports



Search Query reporting



Date & Time	User	Source IP	URL/Domain	Referrer URL	Destination...	Group	Category	Action
10/27/17 11:12 AM	jdoe	10.128.16.1...	iboss		84.245.40.1...			Allowed
10/27/17 11:07 AM	jdoe	10.128.16.1...	dictionary		28.49.12.189			Allowed
10/27/17 10:00 AM	jdoe	10.128.16.1...	iboss		81.62.90.62			Allowed
10/27/17 9:44 AM	jdoe	10.128.16.1...	drugs		248.42.178....			Blocked
10/27/17 9:08 AM	jdoe	10.128.16.1...	google		113.35.0.161			Allowed
10/27/17 8:37 AM	jdoe	10.128.16.1...	iboss		84.245.40.1...			Allowed
10/27/17 8:21 AM	jdoe	10.128.16.1...	weather		149.65.189....			Allowed

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

iboss produces weekly blogs and other media regarding online safety and current threat vectors, along with advice to keep networks and their users safe.

[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	Simon Eappariello
Position	Senior Vice President Product & Engineering, EMEIA
Date	25.6.18
Signature	*S. Eappariello*