Appropriate Filtering for Education settings

September 2019

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	AdEPT Education (Previously Atomwide Ltd)
Address	2 - 3 Ravensquay Business Centre, Cray Ave, Orpington, BR5 4BQ
Contact details	James Ing
Filtering System	WebScreen™ (incorporating Netsweeper and Fortinet technologies)
Date of assessment	30/10/2019

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		Both of AdEPT Education's underlying service technology providers for WebScreen™ (Netsweeper & Fortinet) are IWF members. For this reason, and hence the facility those memberships already provide, AdEPT Education is not also an IWF member in its own right at this time.
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Yes. The IWF CAIC list is implemented via the Netsweeper component within WebScreen. The IWF functionality is not exposed in the admin user interface and cannot be disabled. Also implemented for all WebScreen users, is the IWF Hash List, a technology which uses Microsoft Photo DNA to apply a unique 'hash' (a sort of digital fingerprint) to an image representing child abuse, that can then be used to identify and defeat other instances of any such image from being propagated around the internet.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Yes. The Home Office Counter Terrorism Internet Referral Unit (CTIRU) block list is applied to WebScreen™ directly by AdEPT Education, as the producer of the filtering service, and is updated upon receipt of any changes received from the Home Office.

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.		WebScreen™ categorises content into one, or multiple 'distinct' categories, which may (or may not, subject to other local or regional legal obligation or precedent) then be 'Blocked' or 'Allowed' by whole category (or categories), or individual URL(s), by each subscribing customer establishment, using single or multiple distinct 'Policies' as best suited to the needs of their establishment and its users Sites unequivocally identified as being 'Illegal', in the context of any subject matter, are automatically categorised and 'Blocked' accordingly at service provider level. Discriminatory content may be identified and categorised through a number of different category definitions according to the subject material it is closest to. Identified sites can also be locally re-categorised for any customer whose view of a resource differs from the default categorisation in such a manner that the default is still felt appropriate for other users. Clear guidance is offered to establishment representatives over the 'Allowed' inclusion of any other 'potentially' inappropriate, or otherwise 'high risk' sites or categories.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		WebScreen™ categorises content into one, or multiple 'distinct' categories, which may (or may not, subject to other local or regional legal obligation or precedent) then be 'Blocked' or 'Allowed' by whole category (or categories), or individual URL(s),

			by each subscribing customer establishment, using single or multiple distinct 'Policies' as best suited to the needs of their establishment and its users. Sites unequivocally identified as being 'Illegal', in the context of any subject matter, are automatically categorised and 'Blocked' accordingly at service provider level. WebScreen offers multiple drug-related categories. Whilst the most obvious ones containing sites promoting or exhibiting the use of illegal drugs, or other instances of substance abuse, are invariably blocked by customers, these can be made available to specific users where there is genuine rationale and value, perhaps to illustrate a specific topic, hazard or argument. Several other categories covering prescribed drugs, drug legislation and legitimate drug use, and drugs within a wider medical or medicinal context, are also available, providing much needed granularity to a complex topic. As with others, identified sites can be locally re-categorised for any customer whose view of a resource differs from the default categorisation in such a manner that the default is still felt appropriate for other users. Clear guidance is offered to establishment representatives over the 'Allowed' inclusion of any other 'potentially' inappropriate, or otherwise 'high risk' sites or categories.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		WebScreen™ categorises content into one, or multiple 'distinct'

			categories, which may (or may not, subject to other local or regional legal obligation or precedent) then be 'Blocked' or 'Allowed' by whole category (or categories), or individual URL(s), by each subscribing customer establishment, using single or multiple distinct 'Policies' as best suited to the needs of their establishment and its users. Sites unequivocally identified as being 'Illegal', in the context of any subject matter, are automatically categorised and 'Blocked' accordingly at service provider level. Web sites offering extremist views, and the promotion of terrorism and terrorist activity are principally identified through the 'police assessed' list which was created for, and is applied on behalf of, the Home Office (CTIRU). Other categories may be used to identify 'lesser' assessed sites through their references to a range of items including violence, hate speech, criminal activity, and the creation or use of weaponry. As with others, identified sites (excluding those from the CTIRU list) can be locally re-categorised for any customer whose view of a resource differs from the default categorisation in such a manner that the default is still felt appropriate for other users. Clear guidance is offered to establishment representatives over the 'Allowed' inclusion of any other 'potentially' inappropriate, or otherwise 'high risk' sites or categories.

Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		WebScreen™ categorises content into one, or multiple 'distinct' categories, which may (or may not, subject to other local or regional legal obligation or precedent) then be 'Blocked' or 'Allowed' by whole category (or categories), or individual URL(s), by each subscribing customer establishment, using single or multiple distinct 'Policies' as best suited to the needs of their establishment and its users. Sites unequivocally identified as being 'Illegal', or a 'network security' risk, are automatically categorised and 'Blocked' accordingly at service provider level. Malware and hacking covers a very wide range of hazards on the internet, especially for schools. WebScreen deploys, or integrates with, a wide range of tools in addition to the use of several categories and default policies. Categories dedicated to the subject are focussed on sites promoting, providing, describing, or advocating computer hacking; filter bypass technologies such as Proxy Anonymizers; computer-related criminal activity or misuse (including the commissioning or carrying out of 'DDoS' – Distributed Denial of Service attacks); the distribution, harbouring or production of virus and malware applications; and Adware. In addition, the categorisation of, and hence access to, the plethora of 'inbound' network remote access applications, including 'conferencing services' containing remote desktop takeover tools, and commercial network management services, is

			comprehensively 'ring-fenced'. Whilst still available if desired, additional controls are applied to these sites to ensure customers do not inadvertently fall foul of apparently innocent services being used inappropriately. This particular aspect of filtering typically integrates closely with other locally deployed services and protocols, such as anti-virus strategies, and diligent firewall management. Clear guidance is offered to establishment representatives over the 'Allowed' inclusion of any other 'potentially' inappropriate, or otherwise 'high risk' sites or categories. In this context, additional guidance may typically cover local acceptable use policies; risk assessment surrounding particular types of site or category; and best practice use of firewall rules and suitable 'protocols'.
Pornography	displays sexual acts or explicit images		WebScreen™ categorises content into one, or multiple 'distinct' categories, which may (or may not, subject to other local or regional legal obligation or precedent) then be 'Blocked' or 'Allowed' by whole category (or categories), or individual URL(s), by each subscribing customer establishment, using single or multiple distinct 'Policies' as best suited to the needs of their establishment and its users. Sites unequivocally identified as being 'Illegal', in the context of any subject matter, are automatically categorised and 'Blocked' accordingly at service provider level.

			Whilst a relatively straightforward challenge in comparison to some others, the wider context of 'Adult content' can extend beyond pornography, and may impact or influence the allowed use of social networking, adult gaming, dating, and other associated categories of site in some situations. Clear guidance is offered to establishment representatives over the 'Allowed' inclusion of any other 'potentially' inappropriate, or otherwise 'high risk' sites or categories.
Piracy and copyright theft	includes illegal provision of copyrighted material		WebScreen™ categorises content into one, or multiple 'distinct' categories, which may (or may not, subject to other local or regional legal obligation or precedent) then be 'Blocked' or 'Allowed' by whole category (or categories), or individual URL(s), by each subscribing customer establishment, using single or multiple distinct 'Policies' as best suited to the needs of their establishment and its users. Sites unequivocally identified as being 'Illegal', in the context of any subject matter, are automatically categorised and 'Blocked' accordingly at service provider level. This subject matter typically falls into two broad camps, those being the conventional web sites advocating, supporting and facilitating piracy and copyright infringement, and those enabling the sharing of content and other resources illegally via Peer2Peer and similar sharing. Multiple categories within WebScreen™ focus on the specific areas closely, and as with virtually all

			others, local re-categorisation of sites can be applied by individual schools. A WebScreen™ category, 'Piracy', contains a list of URLs obtained from the Police Intellectual Property Crime Unit (PIPCU), a department of City of London Police. The 'Infringing Website List', as it's named by PIPCU, contains URLs which have been identified by the Unit as containing copyright infringing material. This list is updated within WebScreen™ upon receipt of any changes. The WebScreen™ category 'Piracy' is 'Blocked' accordingly at service provider level and cannot be disabled. Clear guidance is offered to establishment representatives over the 'Allowed' inclusion of any other 'potentially' inappropriate, or otherwise 'high risk' sites or categories.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		WebScreen™ categorises content into one, or multiple 'distinct' categories, which may (or may not, subject to other local or regional legal obligation or precedent) then be 'Blocked' or 'Allowed' by whole category (or categories), or individual URL(s), by each subscribing customer establishment, using single or multiple distinct 'Policies' as best suited to the needs of their establishment and its users. Sites unequivocally identified as being 'Illegal', in the context of any subject matter, are automatically categorised and 'Blocked' accordingly at service provider level.

			The specific category within WebScreen of 'Extreme' is dedicated to identifying self-harm sites, and those containing other content that may prove harmful to children. Clear guidance is offered to establishment representatives over the 'Allowed' inclusion of any other 'potentially' inappropriate, or otherwise 'high risk' sites or categories.
Violence	Displays or promotes the use of physical force intended to hurt or kill		WebScreen™ categorises content into one, or multiple 'distinct' categories, which may (or may not, subject to other local or regional legal obligation or precedent) then be 'Blocked' or 'Allowed' by whole category (or categories), or individual URL(s), by each subscribing customer establishment, using single or multiple distinct 'Policies' as best suited to the needs of their establishment and its users. Sites unequivocally identified as being 'Illegal', in the context of any subject matter, are automatically categorised and 'Blocked' accordingly at service provider level. In the widest context, violence-related web sites and materials cover a broad spectrum, and as such WebScreen uses several different categorisations to help identify and manage sites accordingly, including 'Violence'; 'Hate Speech'; Extreme; and Criminal Skills. Clear guidance is offered to establishment representatives over the 'Allowed' inclusion of any other 'potentially' inappropriate, or otherwise 'high risk' sites or categories.

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

WebScreen™ utilises the strengths of its underlying technology partners, Netsweeper and Fortinet, but then expands those strengths, and regionalises the results, so that they better suit the UK education sector.

To expand on the capabilities described elsewhere in this response, WebScreen™ offers the following:

Extra 'localised' and specialist web site categories not typically found in business-focused filtering, offering better compatibility with schools' needs.

A devolved hierarchy of central/local policies, that can be adopted and then modified by the local establishment to best suit its particular circumstances, or used in their default state for those with no need or desire to localise the filtered experience.

Support for an innovative access management solution to assist schools wishing to utilise YouTube video resources without needing to allow students access to the whole site's content. Working as one component of the solution, alongside sophisticated network DNS management, and the myVideos module available as part of AdEPT Education's myUSO user portal, WebScreen™ allows school staff to easily identify, pre-select and securely share YouTube resources via myVideos. Pupils can then access the shared videos without the school needing to allow general access to YouTube directly. With myVideos typically protecting younger pupils, older students and/or staff can still be provided with full access to YouTube via conventional WebScreen filter policies if deemed appropriate.

Data Controller authorisation, which is sought for certain 'high risk' categories, in order to ensure that a full awareness exists within (for instance) a school's Senior Leadership Team, of any policies being deployed that may represent a higher risk than is typically deemed acceptable in a school.

Highly granular settings can enable filtering policies to differentiate between such status as staff and students, locations, times of day, the nature of physical and wireless connections, specific devices by type or unique ID, and can also conveniently accommodate USO account-holding visitors from other establishments, or non-USO account holding 'Guests' via a range of options.

The service is extremely well documented, and transparent (except where negated by legal or other obligation) in its application of site categorisation and policy application, management and governance.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy.

Internet history data is stored for the time period 'current academic year + 1' with the academic year being defined from the 1st September to the following 31st August. This data is required to not only allow customers to run reports but to support potential enquiries received by law enforcement agencies.

More information on our retention policies, including WebScreen's, can be seen in the "London Grid for Learning (LGfL) retention and disposal schedule for information stored in Atomwide systems' document, available here.

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

WebScreen™'s content categorisation is a continuous ongoing process, supported by Netsweeper global URL lists and automated AI (artificial intelligence), and underpinned by UK-regionalised categorisation obtained using 'crowd-sourced' intelligence from within its own user community. Local control of policies is actively encouraged, while guidance is provided regarding the need for a balanced approach to filtering being combined with practical and informed support from staff, and the issues that can be encountered by establishments being either too open or too zealous within any given filtering policy. Where policies are deemed to be effectively appropriate, but needing occasional or temporary exceptions to be applied due to changes in circumstances, WebScreen™ policies can be readily modified, and later returned to their otherwise normal state.

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		WebScreen™ default filter policies are applied appropriate to the underlying nature of a filtered establishment (i.e. Primary School, Secondary School, Teachers' Centre, etc.). Per User filtering is available for deployment across all customer establishments. Multiple filtering policies can be applied, in order to recognise the age and needs of different groups of users, or locations, or times of day, and/or combinations of each of the above. Filtering policies can be tailored to respond accordingly to different

		groups of identified individual users, or even a single user.
● Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS.		To an extent, the circumvention issue is bi-directional, with inbound and outbound threats requiring quite different approaches, as are exampled below. In particular, and mostly for outbound traffic, usage of a commercial, public, or even DIY proxy service is countered through the recommended blocking of the 'Proxy Anonymizer' category, which identifies 'advice' sites as well as active proxies, including some 'translation' sites, and other sites that may be represented as being something other than their true underlying nature. For inbound traffic, the most common threat or challenge is from remote access (or remote desktop) services, especially those embedded (whether innocently or not) within other services for which that is not the primary function (such as video conferencing or training services). A range of management guidance and technical recommendations are available to aid establishments gain access to legitimate services safely without unintentionally compromising their local security and/or Acceptable Use policies. In both the above scenarios, and more widely, effective

		firewall management may also play a key role in the application of appropriate controls, including the support or denial of VPN connections, inter-connected web services, and data service synchronisations. Where AdEPT Education also provides managed connectivity and/or firewalling services, these are integrated directly with WebScreen™ from within the online management portal. WebScreen™ filters based on URL & not DNS, therefore the use of DNS over HTTPS does not present a risk of users circumventing WebScreen™ filtering.
● 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, WebScreen™ is fully configurable by appropriately authorised local establishment contacts, or their contracted support agents, via an online portal available 24x7.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Yes, WebScreen™ categorises in excess of 130 distinct content categories, with descriptions of the purpose and summarised content of each, and where appropriate, the implications of enabling access and/or the prerequisites for gaining or enabling access.
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Where WebScreen™ is deployed across a multi-site estate, such as a Multi Academy Trust (MAT), an LA, or similar group of autonomous or semi-autonomous establishments

		needing to be operated or supported centrally, or at least have this as an option, WebScreen's online management portal allows sites to be grouped in a number of different ways to suit different management structures. From within the portal, appropriately authorised administrators can manage individual site policies, as well as setting 'global' rules and policies across all sites within the group. In addition to the online portal, the AdEPT Education Service Desk staff are well versed in dealing with grouped establishments, and are also able to provide advice to existing sites preparing to join or form a Group for the first time.
• Identification - the filtering system should have the ability to identify users		WebScreen™ is fully integrated with AdEPT Education's Shibboleth-compliant IdP, referred to as Unified Sign On (USO). The system therefore recognises any user presenting a USO ID in response to a filtering policy generated request. WebScreen™ also offers 'AD linked filtering'. Where this is used, the system will identify users by Active Directory username.
• 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		WebScreen™ filters any content accessed by http and https protocols, regardless of whether content is browser or application (app) accessible,

via mobile and app technologies (beyond typical web browser delivered content)		and is equally applicable to 'mobile' content accessed via an establishment's filtered infrastructure. WebScreen™ can optionally be deployed with additional content controls relating specifically to mobile apps. For apps carrying non-http or https traffic, and which are hence encrypted or 'hidden' against 'content filtering' (a problem even the UK Government and the wider world is currently grappling with), AdEPT Education's integration of the Fortinet Application Control Service means WebScreen™ can identify specific apps, or categories of app, analyse the type of content and its collective impact on the local infrastructure, and then where necessary, allow, block or otherwise restrict access according to the wider overall policy or policies applied to the establishment as a whole. With the flexibility to be applied to one or more student and staff user groups, and even to individuals, this adds a significant dimension over purely http/https filtering, and is hence well suited to combating threats in the areas of terrorism, cyber-bullying, and grooming, where apps may attempt to take advantage of this 'invisibility'.
● Multiple language support – the ability for the system to manage relevant languages		Yes, via the Netsweeper embedded technology,

		WebScreen™ supports multi-language filtering.
• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		WebScreen's filtering is applied at the network level, and local installed software is not required on client devices, including both wired and wireless connections, to be filtered.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		Yes, via the online management portal, the option to suggest global re-categorisation, or request local re-categorisation, of an individual site or URL, is available to appropriately authorised local establishment contacts, or their contracted support agents.
• Reports – the system offers clear historical information on the websites visited by your users		

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

AdEPT Education, and its customer ISPs (such as, but not limited to, LGfL/TRUSTnet) typically include a wide range of training and support elements with their provision of WebScreen™. Customer ISPs and individual schools, also have the ability to influence and adapt the mode of delivery to suit specific circumstances, and to specify WebScreen's modes of functionality and the default levels of protection applied.

The wider subject of safeguarding support, including at a curriculum level, may be offered either directly by the customer ISP, or indirectly, such as due to association with NEN (The Education Network), and hence a schools' licensed or open access to these resources.

The AdEPT Education Service Desk provides extensive support for both the technical deployment and ongoing management of WebScreen™, and also comprehensive published and direct guidance regarding the 'cultural' usage of it within an establishment, and the implications for and against the deployment of certain policies. Training courses are regularly provided, free of charge, to appropriately authorised local establishment contacts, or their contracted support agents.

[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	James Ing
Position	Product Manager
Date	30/10/2019
Signature