Appropriate Filtering for Education settings

June 2016

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*"[1]. Furthermore, the Department for Education published the revised statutory guidance 'Keeping Children Safe in Education'[2] in May 2016 (and active from 5th September 2016) for schools and colleges in England. Amongst the revisions, 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 college's 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*."

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	London Grid for Learning Known as LGfL, TRUSTnet or LGfL TRUSTnet
Address	LGfL, CI Tower, St George's Square, New Malden, KT3 4TE
Contact details	020 82 555 555 (option 9)
Filtering System	WebScreen™ 2.0 (incorporating NetSweeper and Fortinet technologies)
Date of assessment	17 June 2016

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.	

[1] Revised Prevent Duty Guidance: for England and Wales, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

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

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		WebScreen™ 2.0, the internet filtering solution applied to the LGfL TRUSTnet network, uses URL filtering from NetSweeper and Fortinet, which are both IWF members. Furthermore, LGfL is currently exploring closer partnership working with the IWF.
• and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)		The IWF CAIC list is actively implemented by NetSweeper. This is an always-on feature to comply with legislation and ensure safeguarding for school staff and students – it cannot be turned off by schools.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		This is applied to WebScreen™ 2.0 directly by our support partner Atomwide. This is an always-on feature to comply with legislation and ensure safeguarding for school staff and students – it cannot be turned off by schools.

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.		LGfL's WebScreen™ 2.0 filtering product categorises web content into one or more distinct categories (see Appendix 1), which may (or may not, subject to other local or regional legal obligation or precedent) then be blocked or allowed according to the assigned category/ies, individual URL/s, or the policies defined by the school. Websites unequivocally identified as illegal or a network security risk are automatically categorised and blocked. This cannot be changed by a school. Where a website has been established as potentially inappropriate, however, or if it falls into a high-risk or other category which is blocked by default, a school may take an informed decision to allow these sites in one or more policies. This might be to enable discussion of certain themes in lessons, or where a site's appropriateness may depend upon the age and maturity of users.

			A range of appropriate, balanced default policies are available to suit the typically differing requirements of primary and secondary schools, for both staff and students, which local school administrators can then modify, by blocking or allowing further categories, websites and webpages, and even applying different profiles to different times of day, different logins, or different computers (e.g. Facebook for teachers but only after 3pm, YouTube for pupils at lunchtime, etc.). The default policies are there to enable informed and proactive safeguarding decisions. Free training courses are offered to all schools to help them best understand and manage the filtering / policy system and interface. Alternatively, an authorised Nominated Contact can request individual category blocking / unblocking requests via the LGfL Support Site. LGfL also has a dedicated Safeguarding Board which works on reviewing the filtering systems from a purely safeguarding perspective. The Board also develops keyword lists based on the latest best-practice and school experience, to aid with up-to-date school-safe and school-appropriate filtering. These keyword lists are added as a further layer over the Google Safe Search functionality, which is turned on by default for all schools. Google's YouTube service is available in the modes: open, moderate restricted and severe restricted. All LGfL default to 'severe-restricted' mode, which is recommended. However, schools are permitted to change their settings to use YouTube in 'moderate-restricted' mode. Any school wanting to turn off restricted mode altogether is warned that this is highly inadvisable in an education setting – however, with the approval of the Headteacher, they may bypass DNS settings in order to do so. As part of LGfL TRUSTnet's remit to support education in schools, the online-safety portal os.lgfl.net provides a collated and curated portfolio of resources to help teachers, managers, parents and children learn to become effective and safe digital citizens. Many of these resources

			reflect the management of, rather avoidance of risk, in recognition of the dangers of overblocking. Resources are drawn from the entire online-safety community and a variety of providers, but two LGfL resources are particularly relevant in relation to the balancing act of safeguarding vs overblocking: 'Counter-Extremism: narratives and conversations' deals with specific online threats from exposure to extremist material and potential grooming; 'Trust Me' (developed in partnership with Childnet) aims to engender critical-thinking skills in Primary and Secondary pupils about their online experiences (contact, content and propaganda).
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		See above
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		See above
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		See above
Pornography	displays sexual acts or explicit images		See above
Piracy and copyright theft	includes illegal provision of copyrighted material		See above
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		See above
Violence	Displays or promotes the use		See above

	of physical force intended to hurt or kill		

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

WebScreen™ 2.0 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™ 2.0 offers:

Extra 'localised' and specialist web site categories not typically found in commercial filtering, and 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.

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 polices being deployed that may represent a higher risk than is typically deemed acceptable.

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 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.

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

WebScreen™ 2.0'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™ 2.0 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™ 2.0 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 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.
• 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, 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™ 2.0 categorises 121 distinct content categories, with descriptions of the purpose and summarised content of each, and where appropriate, the implications of access, and/or prerequisites for gaining access.

● Identification - the filtering system should have the ability to identify users		WebScreen™ 2.0 is fully integrated with the LGfL Shibboleth-compliant IdP, referred to as Unified Sign On (USO), which is run by support partner Atomwide. The system therefore recognises any user presenting a USO ID in response to a filtering policy generated request.
● Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies		WebScreen™ 2.0 filters any content accessed by http and https protocols, regardless of whether content is browser or application (app) accessible, and is equally applicable to 'mobile' content accessed via an establishment's filtered infrastructure.
● Multiple language support – the ability for the system to manage relevant languages		Yes, via the NetSweeper embedded technology, WebScreen™ 2.0 supports multi-language filtering.
● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		No local installed software, nor additional hardware, is required for client devices connected to an establishment's filtered infrastructure.
● 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		Yes. A comprehensive range of scheduled, and ad hoc, usage reports is available from the online-management portal, for use by appropriately authorised local establishment contacts, or their contracted support agents.

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*".[3]

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

Free training courses are offered to all schools to help them best understand and manage the filtering / policy system and interface. Alternatively, an authorised Nominated Contact can submit individual category blocking / unblocking requests via the LGfL Support Site.

LGfL also has a dedicated Safeguarding Board which works on reviewing the filtering systems from a purely safeguarding perspective. The Board also develops keyword lists based on the latest best-practice and school experience, to aid with up-to-date school-safe and school-appropriate filtering.

As part of LGfL TRUSTnet's remit to support education in schools, the online-safety portal os.lgfl.net provides a collated and curated portfolio of resources to help teachers, managers, parents and children learn to become effective and safe digital citizens. Many of these resources reflect the management of, rather avoidance of risk, in recognition of the dangers of overblocking.

Resources are drawn from the entire online-safety community and a variety of providers, but two LGfL resources are particularly relevant in relation to the balancing act of safeguarding vs overblocking: 'Counter-Extremism: narratives and conversations' deals with specific online threats from exposure to extremist material and potential grooming; 'Trust Me' (developed in partnership with Childnet) aims to engender critical-thinking skills in Primary and Secondary pupils about their online experiences (contact, content and propaganda).

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

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

- 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	John Jackson
Position	Chief Executive Officer
Date	20 June 2016
Signature	

Appendix 1 – web filtering category list as of 20 June 2016

Please note that this list is subject to change and that definitions of each category and the type of websites likely to be categorised accordingly can be found on the LGfL support site under the WebScreen™ 2.0 menu.

Abortion - Prochoice
Abortion - Prolife
Abortions
Activist/Advocacy Groups
Adult Content
Adult Image
Advertising
Adware
Alcohol
Alternative Lifestyles
Arts & Culture
Bad Link
Banner/Ad Servers
Blogging
Bullying
Classifieds
Computer Security
Criminal Skills
Culinary
Directory
Drugs - Debate
Drugs - Illegal
Drugs - Prescribed
Education
Educational Games
Email
Entertainment
Environmental
Extreme
File Sharing
Forums
Freeware Downloads
Gambling
Games
Gay & Lesbian Issues
General
General News
Hate Speech
Host is an IP
Humor
Images
Infected Hosts
Instant Messaging (IM)
Internet Auction
Intimate Apparel
Intranet Servers
Investing
Job Search
Journals and Blogs
Legal
Malformed URL
Match Making
Matrimonial
Media Protocols
Medical
Medication
Misc Protocols
Music Downloads
Network Unavailable
New URL
No Text
Nudity
Occult
Online Sales
Open Resource Sharing
Parked
Pay to Surf
Peer to Peer
Phishing
Phone Cards
Political
Portals
Profanity
Proxy Anonymizer
Real Estate
Redirector Page
Religion
Ringtones
Safe Search
Sales
Search Engine
Search Keywords
Security Threat
Self Help
Sex Education
SMS Messaging
Social Issues and Support
Social Networking
Sport - Hunting and Gun Clubs
Sports
Streaming Media
Substance Abuse
Tasteless/Illegal/Questionable
Technology
Tobacco
Travel
Under Construction
URL Translation
Violence
Viruses
Voice Over IP (VOIP)
Weapons
Web Chat
Web E-mail
Web Hosting
Web Storage
Web-Based Chat & Email