Appropriate Filtering for Education settings

June 2021

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*" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's 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."

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	LGfL
Address	9th Floor, 10 Exchange Square, Primrose Street, London, EC2A 2BR
Contact details	safeguarding@lgfl.net
Filtering System	**WebScreen** (https://webscreen.lgfl.net) and **HomeProtect** (https://homeprotect.lgfl.net) products for network and remote filtering, respectively (both based on Netsweeper technologies; other Netsweeper variants may at times be available)
Date of assessment	18 October 2021

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		LGfL is an active member of the IWF and sits on the IWF Funding Council to help shape and inform this vital institution.
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		This list is implemented for all our filtering customers and cannot be bypassed. Even the very few customers which require a raw internet feed without filtering still cannot access sites on the IWF blocklist. We also go beyond the IWF URL list in that the IWF's Image Hash List is also enforced by the Netsweeper engine on which all our filtering is based. This ensures any sites are blocked which may be hosting new instances of child sexual abuse images that have been reuploaded onto a new website in order to avoid a block.
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		This list is also implemented for all our filtering customers and cannot be bypassed.

Further illegal content blocked by LGfL:

LGfL was the first UK internet service provider to implement the City of London Police's Infringing Website List (IWL) from the Police Intellectual Property Crime Unit (PIPCU). This blocklist contains websites which have been proven to include illegal pirated content (such as Hollywood films). Each site has been independently verified as containing illegal content by a police officer. The list is particularly useful for schools as these sites are not only often linked to criminal gangs, but often include malware, so it is important to protect staff and students form the illegal material and potential viruses and security breaches. What is more, schools may otherwise be held to account for breach of copyright if this material is downloaded on their network, leading to thousands of pounds of fines from the copyright owners.

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.		As with all categories listed here, combatting this category cannot be achieved through blocking alone, and it is crucial that education forms part of the same conversation as filtering and blocking. Safe search can be enforced in search engines and the moderate or strict restricted DNS modes within YouTube help to remove many videos which are inappropriate for children that fall into this or any other of the categories listed here. Schools can choose to whitelist a site that is in an otherwise blocked category, or block a site from an otherwise allowed category (and do this per group/IP/time etc). This category of discrimination is most likely to be covered by the category of Hate Speech. See also Extremism section below for education support.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		See above for general notes. Schools can choose to block or allow three categories relating to drugs debate, illegal drugs and prescription drugs.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		See above for general notes. There is a violence and extremism category into which many of these sites will fall and on which schools can compile ad hoc or custom reports (as with any other category). This is in addition to the CTIRU Home Office terrorist block list as described on the previous page. LGfL also does a lot of education work in this area which can be viewed via prevent.lgfl.net including a new joint resource with the DfE to support critical thinking for safeguarding, including but not limited to Prevent, called Going too Far (goingtoofar.lgfl.net).
Malware / Hacking	promotes the compromising of systems including anonymous browsing and		See above for general notes.

	other filter bypass tools as well as sites hosting malicious content		This may relate to our categories of viruses/infected hosts. It is further supported by the PIPCU list (see back 1 page) and other LGfL technologies beyond the core filtering service which are offered to all our schools, such as Sophos, Malwarebytes and others.
Pornography	displays sexual acts or explicit images		See above for general notes. Further to this we provide support and signposting at pornography.lgfl.net
Piracy and copyright theft	includes illegal provision of copyrighted material		See above for general notes. There is a Netsweeper category for Piracy but also the PIPCU blocklist is applied as per the notes on the previous page.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		See above for general notes. Self-harm sites will usually fall into the 'extreme' category. They may be blocked by site theme or by keyword, either by the Netsweeper classification engine or LGfL keywords. The collection of resources at bodyimage.lgfl.net may be helpful further support in this area for schools.
Violence	Displays or promotes the use of physical force intended to hurt or kill		See above for general notes. This may fall into the categories of violence/extreme/web storage/criminal/adult. LGfL education support in this area includes countylines.lgfl.net, syv.lgfl.net and survive.lgfl.net.

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

The categories which exist for granular block/allow rules can be applied to different users, groups, times, IP ranges, etc within WebScreen and HomeProtect; they are listed below this box for information. Users can see definitions of each category within the portal. They can be applied at a school or MAT/LA level for user groups (per Active Directory or USO login), and/or by time or IP address. 'Bundles' also exist to allow groups of URLs to be treated together, either because a school or MAT wishes to group regular websites or for those such as the LGfL Facebook bundles which includes the 6 or 7 different web addresses which must work in order for the facebook site to work (and vice versa).

Further detail and videos guides for different aspects of the in-school system and its functionality can be found at https://webscreeninfo.lgfl.net and for our remote offering at http://homeprotect.lgfl.net.

Data Controller authorisation is sought for certain 'high risk' categories (e.g. sites which can be used as a proxy and therefore might be used to avoid blocks), 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.

Please note that https decryption is available to increase the sophistication of filtering. By way of explanation, without decryption, any site that begins with https:// (nearly 60% of all the world's websites) is blocked or allowed at domain level (e.g. https://www.bbc.co.uk can be blocked or allowed as a whole website); however, with decryption a school can block or allow an individual page, e.g. block or allow a section or page within a website, e.g. block https://www.bbc.co.uk**/iplayer** but allow https://www.bbc.co.uk**/news**).

WebScreen categories:

Abortion - Prochoice
Abortion - Prolife
Abortions
Activist/Advocacy Groups
Ad Blocking
Adult Content
Adult Image
Advertising
Adware
Alcohol
Alternative Lifestyles
Arts & Culture
Bad Link
Banner/Ad Servers
Blogging
Bullying
Business
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
Humour
Images
Infected Hosts
Instant Messaging (IM)
Internet Auction
Intimate Apparel
Intranet Servers
Investing
Job Search
Journals and Blogs
Legal
Malformed URL
Malicious Web Obfuscation
Malware
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
Piracy
Political
Portals
Privacy
Profanity

Proxy Anonymizer
Real Estate
Redirector Page
References
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
Vehicles
Violence
Viruses
Voice Over IP (VOIP)
Weapons
Web Chat
Web E-mail
Web Hosting
Web Storage
Web-Based Chat & Email

For HomeProtect these categories are slightly different:

Abortions
Ad Blocking
Adult Mixed Content
Advertising
Adware
Age Restriction
Alcohol
Arts and Culture
Body Modification
Bullying
Business
Child Erotica
Child Sexual Abuse
Classifieds
Content Server
Copyright Infringement
Criminal Skills
Culinary
Directory
Education
Educational Games
Entertainment
Environmental
Extreme
Financial Services
Gambling
Games
General
General News
Government
Hacking
Hate Speech
Health
Host is an IP
HTTP Errors
Humor
Images
Infected Hosts
Intimate Apparel
Intranet Servers
Job Search
Journals and Blogs
Legal
Lifestyle Choices
Malformed URL
Malicious Web Obfuscation
Malware
Malware Hosts
Marijuana
Match Making
Matrimonial
Medication
Military
Network Timeout
Network Unavailable
New URL
No Text
Nudity
Occult
Open Mixed Content
Parked
Pay to Surf
Payment Gateway
Peer to Peer
Phishing
Phishing Hosts
Phone Cards
PIPCU
Pornography
Portals
Privacy
Profanity
Real Estate
Redirector Page
References
Religion
Remote Access Tools
Safe Search
Sales
Search Engine
Search Keywords
Self Harm
Sex Education
Social Networking
Sports
Streaming Media
Substance Abuse
Technology
Terrorism
Tobacco
Translation
Travel
Under Construction
Vehicles
Viruses
Weapons
Web Chat
Web Email
Web Hosting
Web Proxy
Web Storage

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to the identification of individuals and the duration to which all data is retained .

System logs for WebScreen are retained for the period of 1 year after the end of the academic year and then disposed of. This not only complies with the Investigatory Powers Act 2016 which requires ISPs to retain this data for 12 months, but also allows schools the opportunity to run investigations after the fact during an extended period. Where these files have been downloaded by a school for a safeguarding record, the school can apply DfE recommended retention periods to the downloaded files. There is no justification for LGfL to retain these logfiles over a longer period without justification, hence the application of this 'academic year-end + 1 year' approach.

The extent to which an individual can be identified by the reports will vary from school to school depending on the extent to which they have set up per-user filtering. Where per user policies are applied, logs and reports will identify usernames allocated by school accounts.

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

- When pupils use their parents' or their own devices at home (as opposed to school managed wones which can have HomeProtect applied), they do not have the protections offered by a schoolsafe connection – often parents are not aware of the basic family protections available on home broadband connections of games consoles and mobile phones. Accordingly, we encourage schools to focus on educating pupils/students about how to use devices and the internet safely and securely, and above all what to do if they see or experience something which worries or harms them or makes them uncomfortable. Strong filtering must go hand-in-hand with strong education and safeguarding at all times to prepare young people for a digital world.
- There is a fine line between under- and over-blocking, and of course this depends on the school, context and specific user. That is why we encourage schools to customise the default strict policy settings we give them when they join – there are templates for primaries and secondaries – according to the needs of the school and its community. With the exception of the illegal content lists, a school can choose to allow or block any category for a particular group/s in line with its own needs and risk assessment.
- This is further supported by the ability to provide different policies for different user groups using Active Directory integration or USO account browser logins (LGfL's Shibboleth-compliant IdP is Unified Sign On or USO), as well as IP and time-based policies to add further flexibility.
- We provide a range of training courses and resources to support teaching young people about how to stay safe online, and this supports the aims of not overblocking but ensuring adequate protections and backing it up with firm policies and educational messaging.
- We encourage schools to make the most of the relationship between filtering and monitoring (LGfL will soon have a new monitoring solution available to its schools and in the meanwhile, many already buy into such a system). The two are important because if you use monitoring to see why a child or young person took a particular route to a piece of content or website, you will learn much more but also be able to have slightly less strict filtering.

- Training on our solutions is not only offered for technical teams, but also via a 20 minute safeguarding shorts session on filtering for safeguarding leads to help them understand what filtering can do and how it can be used as part of a wider contextual safeguarding approach.
- The use of Netsweeper classifications mean that LGfL takes advantage of the artificial intelligence systems used to categories AND constantly reassess sites to ensure overblocking does not take place due to categorisation errors.
- Customisable block pages allow schools to give more information to users about the route to unblock a page and to why it is blocked in the first place.
- We recommend that YouTube is not blocked but that restricted modes are set via DNS, and also provide guidance on how to work within the constraints of the YouTube system to make these more flexible and appropriate at youtube.lgfl.net (recently updated after changes made by Google).

We recommend a graduated approach to exposing children to technology as they develop; an example might be the use of safe search engines with younger pupils rather than relying on the enforced safe search in school that may not be turned on at home; or to having different filtering policies for different year groups. As pupils get older and develop, it is appropriate to relax restrictions and the flexibility of our filtering systems allow this throughout.

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		As detailed in the box above, schools can apply and then customise policy templates to the needs of their users. They can apply these to groups of users (e.g. individual/class/year group, pupil, teaching staff, admin staff, etc) using Active Directory or USO login, or by time and/or IP address. Schools can choose to whitelist a site that is in an otherwise blocked category, or block a site from an otherwise allowed category (and do this per group/IP/time etc). The system is highly flexible to allow schools to exercise their own judgement in line with their expertise, local knowledge and risk assessment.
• 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.		LGfL filtering is not a DNS-based filter, so efforts to circumvent the system using DNS over https or changing DNS server will have no impact on the system. VPNs and Proxy sites can be blocked and classic sites used to bypass filtering such as Google Translate are blocked by default (put into the high-risk category; Headteacher approval can be given to allow the site, but alternatives are available without the potential for use as a proxy anonymiser).

		Safe search can be enforced in search engines. The active management of firewalls also plays a key role in the avoidance of techniques and technologies to bypass protection.
● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		With the exception of illegal sites, schools can change/apply any policy or group or whitelist or blacklist any site regardless of general policy application. They have full control of the system. MATs / LAs can also appoint admins to apply policy changes on behalf of a school where appropriate. The admin portal can be accessed anywhere, anytime, by authorised admins within the school and where appropriate LA/MAT. This applies equally to the WebScreen and HomeProtect portals.
● Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is streamed to the user and blocked. For example, being able to contextually analyse text on a page and dynamically filter		Netsweeper has developed an AI system that is constantly scanning the internet to analyse the content of all websites – it does not simply work at the domain level but is scanning all pages and making ongoing changes to categorisations throughout the day. This is well illustrated by the stats on changes made during the past 24 hours by the Netsweeper categorisation engine at netsweeper.co.uk/live-stats LGfL also recommends the use of monitoring tools to understand more about the journey of young people online and on devices.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		This document can be taken to outline our policy, alongside further details given at webscreeninfo.lgfl.net and YouTube.lgfl.net. Category listings and definitions are also given within the admin portal itself.
● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Local authorities / Multi-academy trusts can make all the same changes that their school admins can make and easily change between the schools they have permission to manage.
● Identification - the filtering system should have the ability to identify users		Where Active Directory or USO login is used, the identification of users for filtering or reporting is by nature easiest. Where a school opts for IP based filtering, reporting will be limited to IP address but can be easily narrowed down to time and behaviour to help identify users. Reporting is very detailed for both regular, scheduled and ad hoc

		reports. Google Directory synch will soon be added to allow further granular per-user rules and filtering (expected 2021/2022).
• 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)		LGfL 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. Where apps use these protocols, filtering works in a similar way to web browser filtering and schools can choose to allow or block each app on a per-app basis. This is best done using a mobile-device management (MDM) system (many LGfL schools use the Meraki licences offered by LGfL). As with all elements of filtering, it is vital that schools also engage with the education side of online safety to equip students for when they are on their family home or mobile connections with little or no filtering.
● Multiple language support – the ability for the system to manage relevant languages		All our filtering benefits from the 46 languages in the Netsweeper dynamic categorisation.
● Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)		WebScreen, the LGfL filtering for school sites, is fully run at the network level and no installation on user devices is required except where https decryption is rolled out – this requires (as for any other provider) the use of certificates to allow the decryption to take place.
● Remote devices – with many children and staff working remotely, the ability for devices (school and/or personal) to receive school based filtering to a similar quality to that expected in school		HomeProtect, the LGfL webfilter for school managed devices deployed for use in the home, is by design a client based filter in order to make sure it filters all internet whether at home, in a café, a library or wherever. It is available for Windows (.msi file), Chrome/Google Workspace (chrome extension), Android and iPad (both via a browser app). Out of the box, schools are asked to choose between 'Safe with Social Media and Gaming Allowed' and 'Safe with Social Media and Gaming Blocked' (given that social media and gaming are the two areas where school approaches vary the greatest, especially for use outside the home). These can then be fully customised according to school needs but the categories and sites are designed to allow the types of sites most likely to be used for homework or remote learning (e.g. all

		video sites are allowed eg iPlayer, YouTube etc as homework is likely to be set this way – instructions on how to set YouTube modes on a device level are shared as part of the installation process). Generally a home policy will be less strict than a school one, hence the defaults take this into consideration, and that most schools will be happy for students to use devices for their own ends, as long as this is possible safely and away from the most harmful sites. However, as before, education is key and parental engagement.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		School admins can report an incorrectly categorised site within the admin portal or flag a site that should be blocked. Errors, queries and other reports can also be filed to our helpdesk.
• Reports – the system offers clear historical information on the websites visited by your users		WebScreen only - detailed reports can be run by admins within the admin portal. These can be scheduled or ad hoc, can be per user/policy group/IP/URL/category group/category. Log files are retained as detailed above for the remainder of the academic year plus 1 year.

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

LGfL's DigiSafe team ensures that the infrastructure and technology we deliver to LGfL schools serves the safeguarding agenda, for example through web filtering (we scan over one billion URLs each day) and mail scanning (two million emails each day). But this is only part of the jigsaw.

We run a national safeguarding centre of excellence to support schools as they keep children safe online and beyond. This support includes live training (safetraining.lgfl.net) and self-service cpd (safecpd.lgfl.net) for staff, support for parents (parentsafe.lgfl.net) blogs, newsletters and social media feeds and other communications to make sure that schools are up to date with legislation and practice.

We operate a resource portal to save teachers time and help them quickly access the best of the support available for pupils, parents and school staff, and we give schools to our expertise through policy templates for them to adapt and apply in their schools.

LGfL also contributes to various national bodies that shape safeguarding policy and practice, inform government and carry out research to ensure that we are always up to speed with the latest threats and opportunities online, e.g. pupil focus groups and pupil surveys.

We work with partners to produce unique materials such as the recent collaboration with the Department for Education 'Going Too Far – Extremism and the Law', a critical thinking resource to help young people understand the law online and not cross it themselves or be sucked in by others trying to mislead or groom them.

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

We also support schools implementing the new online safeguarding focus within the new statutory National Curriculum subject RSHE/PSHE, and continue to support specialist safeguarding areas, such as gangs/youth violence, county lines, incels and MASH referrals. The broader commitment to safeguarding is shown in that all our online support materials are made available open access for the whole education community, such as translations of Keeping Children Safe in Education Part 1 into 10 community languages.

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	Mark Bentley
Position	Safeguarding & Cybersecurity Manager
Date	18 October 2021
Signature