

Appropriate Filtering for Education settings

September 2019

Filtering Provider Checklist Responses

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	LGfL
Address	9th Floor, 10 Exchange Square, Primrose Street, London, EC2A 2BR
Contact details	safeguarding@lgfl.net
Filtering System	WebScreen / Netsweeper / Freedom2Filter
Date of assessment	20 December 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
<ul style="list-style-type: none"> Are IWF members 		LGfL is an active member of the IWF and regularly attends the IWF Funding Council to help shape and inform this vital institution.
<ul style="list-style-type: none"> And block access to illegal Child Abuse Images (by actively implementing the IWF URL list) 		<p>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 blacklist.</p> <p>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.</p>
<ul style="list-style-type: none"> 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 blacklist 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 from 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.		<p>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).</p> <p>This category of discrimination is most likely to be covered by the category of Hate Speech. See also Extremism section below for education support.</p>
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		<p>See above for general notes.</p> <p>Schools can choose to block or allow three categories relating to drugs debate, illegal drugs and prescription drugs.</p>
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		<p>See above for general notes.</p> <p>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.</p> <p>LGfL also does a lot of education</p>

			work in this area which can be viewed via prevent.lgfl.net
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		See above for general notes. 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 offered to all 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

The categories within WebScreen are 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.

Further detail and videos guides for different aspects of the system and its functionality can be found [here](#).

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.

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>).

content and many other aspects.

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

Web-Based Chat & Email

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

System logs 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.

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

- When pupils go home from school they do not have the protections offered by a schoolsafe connection, so we encourage schools to focus on educating pupils/students about how to use devices and the internet safely and securely, but 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.
- 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 due 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](https://www.youtube.com/yt/about/policies/).
- 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. 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
<ul style="list-style-type: none"> Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role 		<p>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.</p> <p>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).</p> <p>The system is highly flexible to allow schools to exercise their own judgement in line with their expertise, local knowledge and risk assessment.</p>
<ul style="list-style-type: none"> 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. 		<p>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).</p> <p>Safe search can be enforced</p>

		<p>in search engines.</p> <p>The active management of firewalls also plays a key role in the avoidance of techniques and technologies to bypass protection.</p>
<ul style="list-style-type: none"> Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content 		<p>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.</p>
<ul style="list-style-type: none"> Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking 		<p>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.</p>
<ul style="list-style-type: none"> Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard 		<p>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.</p>
<ul style="list-style-type: none"> Identification - the filtering system should have the ability to identify users 		<p>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</p>

		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.
<ul style="list-style-type: none"> 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) 		<p>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.</p> <p>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.</p> <p>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.</p>
<ul style="list-style-type: none"> Multiple language support – the ability for the system to manage relevant languages 		All our filtering benefits from the 47 languages in the Netsweeper dynamic categorisation.
<ul style="list-style-type: none"> Network level - filtering should be applied at ‘network level’ ie, not reliant on any software on user devices 		LGfL filtering 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.
<ul style="list-style-type: none"> Reporting mechanism – the ability to report 		School admins can report an incorrectly categorised site

inappropriate content for access or blocking		within the admin portal or flag a site that should be blocked. Errors, queries and other reports can also be filed to our helpdesk.
<ul style="list-style-type: none"> • Reports – the system offers clear historical information on the websites visited by your users 		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 below 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

For schools on the LGfL network, LGfL’s DigiSafe team ensures that the infrastructure and technology we deliver 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 which is both online and beyond. This support includes face-to-face [training](#) and [conferences](#), online [webinars](#) for staff and or [live parent sessions](#), [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 the UK’s largest online safety pupil survey, [Hopes and Streams](#).

In 2019/2020 we are focussing on helping schools to prepare for the new statutory National Curriculum subject [RSHE/PSHE](#), and adding support for safeguarding matters such as [gangs/youth violence](#) and [county lines](#). The broader commitment to safeguarding is shown in that all our online support materials are made available open access for the whole UK 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:

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

- 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	20 December 2019
Signature	