St Martin's C of E Primary School

Filtering and Monitoring Policy

March 2024
Review 2027

Introduction

Schools (and registered childcare providers) 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" (Revised Prevent Duty Guidance: for England and Wales)

Furthermore, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology".

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."

From the information provided to us by our suppliers LGFL and Senso cloud, we are confident that the web filtering solution as configured meets the current DfE guidance (see Appenidx 1 and 2 for our providers' self-certification – as listed on the UK Safer Internet Centre website)

Filtering

At St Martin's:

We have an internet connection which is provided through LGFL (London Grid for Learning), which uses Webscreen filtering (see appendix 1 for their certification).

This means we have a dedicated and secure connection that is protected with their firewall and multiple layers of security, including a web filtering system, which is made specifically to protect children in schools from content such as: pornography, race hatred, gaming, sites of an illegal nature, whilst using our school network. Pupils are not permitted to have access to any personal smart devices – see Mobile Phone Policy.

Chatrooms and social networking sites are blocked sites except those that are part of an educational network or approved Learning Platform.

We only unblock other social networking sites for specific purposes eg Internet Literacy lessons
All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status.

There is no pupil access to music downloads and shopping sites – except those approved for educational purposes.

When pupils are accessing Google Classroom from home, we encourage the use of Google Chrome as the search engine used and the use of the pupil's school login, which enables Google Safe Search.

Staff should not use school devices for their own personal use.

Monitoring

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

1. Physical monitoring

At St Martin's staff are vigilant in its supervision of pupils' use at all times, as far as is reasonable and uses common sense strategies in learning areas where older pupils have more flexible access.

Children are expected to follow our behaviour policy at all times, which includes following instructions. Any breach of this would be dealt with in line with this policy.

2. Internet and Web Access

Staff are expected to have previewed websites before use and are expected to plan the curriculum context to internet use to the pupils' age and ability, using Google Safe Search when searching is required - this is enabled across all devices in school.

When using ipads, pupil and staff use the Senso search facility, which is monitored by Senso software.

3. Active/Pro-active technology monitoring services

At St Martin's we use Senso.cloud to monitor our devices when linked to the school network and all devices loaned to pupils for remote learning. Senso helps to protect our pupils by providing in realtime text analysis, keystrokes, and Artificial Intelligence (AI) to analyse screenshots for visual threats. Their violation libraries are graded into five different levels of severity: Low, medium, high, critical and urgent risk

Senso monitors all activity on devices and logs all websites visited, along with the logging on history for each user and the website visited. Each adult and pupil at St Martin's primary school must log into each device using their own username and must log out again after use. This is to allow the headteacher, deputy headteacher and school business manager to be alerted to any concerning activity and to identify the individual at risk at any time.

Staff must ensure that their password is never shared or written down.

The headteacher, deputy headteacher and school business manager are able to view the full violation log and associated screenshots at any time. In addition, they can also view the screen of any user on a device in real time, although this will only be done when there is a reasonable need to do so. Other DSLs will be emailed any critical and urgent risk alerts, so that they can inform the headteacher or deputy headteacher, but they will not have access to screenshots and the full violation log, in order to protect them from viewing any sensitive or confidential documents.

All devices in school and staff school laptops when used out of school, are monitored and all users are aware of this.

Any safeguarding concerns will be reported to the relevant line manager, these may be logged as low level concerns or escalated to the LADO if necessary.

If a pupil is using a personal device at home, school are unable to monitor or filter their usage. Parents are encouraged to use parental settings on their broadband service and devices in their home which their children can access.

Staff email and CPOMS (our Safeguarding Management System) are not monitored due to the confidential nature of the content, which may be at risk of being viewed and shared.

Content libraries categorise any potential violations, these are: illegal sites eg terrorism, bullying, child sexual exploitation, discrimination, drugs substance abuse, extremism, pornography, self-harm, suicide and violence.

Only the headteacher and deputy headteacher are pro-actively monitoring the alerts and are able to give each a 'status'. In the case of a false positive, it will be recorded as such. The school business manager will have access to these in order to ensure that any violations on the headteacher and deputy headteacher's devices are actioned appropriately.

Actions following a proven concern

Proven concerns from pupils will be recorded on CPOMS via the Senso share capacity. Any actions taken will be recorded and shared with parents and carers, including sharing the screen shot of the violation or wording of concern.

Proven staff violations / concerns may lead to a low level concern being recorded, or a report to the LADO if of a safeguarding concern.

We recognise that some violations and alerts may be linked to a person's mental health and well-being. As a school we are able to offer pastoral support to both adults and pupils in need. This may be via our own in school learning mentors or our Adult and Youth mental health first aiders. We are also able to refer to external agencies.

If the content is a safeguarding concern and the child is at risk of harm – the appropriate agencies will be informed by the DSL or any DDSL in their absence.

Monitoring and reporting to governors

The deputy headteacher will record the number of weekly violations and any concerns on a weekly basis. This will be reported to governors termly via the full governing meeting.

SENSO will be tested monthly to ensure alerts are being received for critical alerts. This is logged in our Online Safety, Filtering and Monitoring One Drive.

Our internet filtering is checked monthly, using testfiltering.com (recommended by the UK safer Internet Centre) to ensure that it is fully protecting us from child sexual abuse content, terrorism content, adult content and offensive language. This is logged on our Online Safety, Filtering and Monitoring One Drive.

Links to other policies
Safeguarding Policy
Online Safety Policy
Online Learning Policy
Mobile Phone Policy
Preventing Extremism and Radicalisation Guidance
Behaviour Policy
Data Protection Policy

Appendix 1 – LGFL Filtering Self Certification

Appropriate Filtering for Education settings

May 2023

Filtering Provider Checklist Reponses

Schools (and registered childcare providers) 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, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self review systems (eg www.360safe.org.uk) that will support a school in assessing their wider online safety policy and practice.

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 regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to [Content, Contact, Conduct, Contract] 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*."

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 and compliance related: safeguarding@lgfl.net Technology queries: schoolprotect@lgfl.net and homeprotect@lgfl.net
Filtering System	SchoolProtect-WebScreen and HomeProtect are our products for network and remote filtering respectively (both based on Netsweeper technologies; other Netsweeper variants may at times be available) Details via filtering.lgfl.net Advice for DSLs via safefiltering.lgfl.net
Date of assessment	July 2022

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 to help shape and inform this vital institution. We sit on the IWF Funding Council where Mark Bentley is currently vice chair.
● 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.
● Confirm that filters for illegal content cannot be disabled by the school		These lists cannot be bypassed or accidentally turned off

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. We offer county lines support and training via countylines.lgfl.net

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).
Gambling	Enables gambling		There is a dedicated gambling section which we would expect all schools to block.
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 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 SchoolProtect-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 from September 23 via Chromebook authentication too), 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).

Proxies and VPNs are handled in their own easily blocked categories.

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**).

Over the summer of 2023 we are rolling out a new system to allow much more widespread decryption for the 23/24 year and are encouraging schools to install certificates in preparation for this.

**** NB, the filtering categories we use are pasted for reference at the end of this document.**

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.

SchoolProtect-WebScreen 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.

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. In September 23 Chromebook authentication will be added for further flexibility and there are plans for more granularity with 365 and other Google logins shortly afterwards.
- 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. Many of our schools receive a monitoring service from another provider. 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. We give more information on the differences between filtering and monitoring and how not to overblock in our information page for DSLs at safefiltering.lgfl.net

- Training on our solutions is not only offered for technical teams, but also via a 30 minute course 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. These help all parties understand the system and the importance of not overblocking.
- 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
● Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff		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. In September 23 Chromebook authentication will be added for further flexibility and there are plans for more granularity with 365 and other Google logins shortly afterwards. 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 DNSbased 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. Google Translate is allowed per se but the function to translate an entire website is blocked as this is a classic way to avoid filtering by translating an adult site, for example. Safe search is enforced by default for google, bing and yahoo and the search engine category can be used to block others. 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. Any changes to the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes		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 SchoolProtect-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, this would include AI generated content. 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 as these tools can monitor text as it is input on the page. Most AI tools are not designed for use by children and extreme care should be taken. There will be soon an AI category and we would recommend this is blocked so that schools can allow AI tools one by one if they choose to do so.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		We would like schools to take this document as our policy, as it outlines our approach to various areas especially overblocking.

		There are further details at WebScreeninfo.lgfl.net https://homeprotect.lgfl.net https://safefiltering.lgfl.net and YouTube.lgfl.net. Category listings and definitions are also given within the admin portal itself. We recommend that schools fully review all settings to ensure it is appropriate and safe for their setting's needs without overblocking. We help them do so with separate training for DSLs and tech teams and our guidance at https://safefiltering.lgfl.net as well as our online safety policy which outlines a whole-school approach and rationale for combining technology, safeguarding, curriculum and more.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Local authorities / Multiacademy trusts can make all the same changes that their school admins can make and easily change between all the schools they have permission to manage for reporting or to make changes. We recommend that bundles/shared lists are used to enforce blocking or allowing across an LA or MAT.
• 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. In September 23, Chromebook authentication will be added for further flexibility and there are plans for more granularity with 365 and other Google logins shortly afterwards.
• 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). Providers should be clear about the capacity of their filtering system to manage content on mobile and web apps		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. Where apps use certificate pinning or different firewall ports and non https/s traffic, we recommend the use of

		MDMs to block use of these apps or adoption of a thirdparty monitoring service to monitoring these in real time.
● 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)		In school, yes the filtering is all network level and so applies to any device used on the network.
● Remote devices – with many children and staff working remotely, the ability for school owned devices to receive the same or equivalent filtering to that provided in school		At home, 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. The can also change policies instantly for their school to allow or block a site. Any errors, queries and other reports can also be filed to our helpdesk. We encourage schools as they do their 'regular checks' under the new standards to set up a mechanism for staff to internally report content that needs to be blocked (or allowed, which is just as important to avoid overblocking).
• Reports – the system offers clear historical information on the websites users have accessed or attempted to access		Detailed reports can be run by admins within the admin portal. These can be scheduled or ad hoc, can be per AD or USO user/policy group/IP/URL/category group/category. Chromebook authentication in September 2023 will enhance this user information further and this

		will soon be enhanced with further authentication systems. Log files are retained as detailed above for the remainder of the academic year plus 1 year.
• Safe Search – the ability to enforce 'safe search' when using search engines		Safe search is enforced by default and we encourage schools to check this as part of their regular check regime.

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 SafeguardED 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) 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.

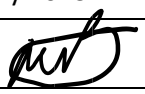
We work with partners to produce unique materials such as the recent collaboration with the Department for Education 'Going Too Far – Extremism and the Law', a critical thinking resource to help young people understand the law online and not cross it themselves or be sucked in by others trying to mislead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

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.

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

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 selfcertification 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 July 2023
Signature	

Please see overleaf for our filtering categories for reference

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

Appendix 2 – Senso Self certification

Appropriate Filtering for Education settings

April 2023

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	Renato Software Ltd.
Address	Sterling House, Wheatcroft Business Park, Edwalton, Nottingham, NG12 4DG

Contact details	0115 857 3776 m.payne@renatosoftware.com
Filtering System	Senso Content Filtering
Date of assessment	20/04/2023

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		Senso is a member of the IWF and actively communicates with them.
● and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		IWF Lists are provided and updated within Senso via an API.
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		CTIRU URL Lists are provided and updated in real time within Senso via an API.

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.			The discrimination category is one of 500+ unique web filtering content categories available to Senso, and includes daily and real-time updates, as well as ActiveWeb traffic from over 600+ million end users globally with 99% ActiveWeb Coverage and Accuracy. The selection of active categories is made based on the needs of our users.

Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances			Several categories combine to cover Drugs and Substance Abuse as above.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance			Extremism is covered as above, plus real-time daily updates of the CTIRU URL lists.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content			Malware and hacking are covered by the Malicious Internet Activity category.
Pornography	displays sexual acts or explicit images			Pornography and adult content are covered by a number of categories.
Piracy and copyright theft	includes illegal provision of copyrighted material			Piracy and copyright theft are covered by the Criminal Activity / Piracy categories.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)			Self-harm is covered by a dedicated self-harm category.
Violence	Displays or promotes the use of physical force intended to hurt or kill			Weapons and violence are covered by dedicated categories.

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

The Senso Content Filtering has the capability to filter against 500+ unique content categories, with more than 99% active web coverage and accuracy. More than 200 languages are supported and it receives daily and real-time updates.

Senso's Content Filtering not only benefits from extensive category-based libraries to block inappropriate websites, but also uses Artificial Intelligence to check the content of every website a student attempts to visit and will proactively include any inappropriate websites within the filtering libraries.

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.

We have a basic filter package which doesn't include logging of internet history, and a premium package which includes logging of internet history. The latter retains logs from the date of installation for the length of a customer's active subscription.

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

Senso as a provider work closely with partners and customers to ensure the filter is appropriately blocking harmful and inappropriate content without over-blocking. Customers have the option to both schedule and turn off completely specific categories such as social media and gaming, based on age or role within the school, to allow for a flexible and strategic approach to internet use. Senso also provides the ability to whitelist any websites which are blocked by Senso Content Filtering on the fly, as required by the individual customer.

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		Senso Content Filtering can: - Schedule all/some categories - Group web-filtered users by criteria such as staff / year group with options to allow certain categories at certain times and have different strengths of filter.
● 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.		Senso blocks access to torrent repositories, proxy anonymisers, and peer-topeer file-sharing sites to help prevent circumvention.
● Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		Senso has the ability to add wildcards, words or URLs to the filter as required. Filter categories can be turned on and off, and URLs can be whitelisted.
● 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		Senso's Content Filtering uses Artificial Intelligence to check the content of every website a student attempts to visit and will proactively include any inappropriate websites within the filtering libraries.
● Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Senso maintains a document which details what content should be in which category, as well as a detailed factsheet on the approach the web filter takes. Senso's Content Filter combines AI with human assessment to maintain over 99% accuracy of web filter categories. The present document can be taken as our rationale on filtering and overblocking.

• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Senso Content Filtering is scalable and flexible to support multi-site management from the top level right down to individual user-specific filtering policies.
• Identification - the filtering system should have the ability to identify users		Users are identified when they log on to the device.
• 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)		Senso Content Filter implements market-leading web filtering across all Chrome-based web apps, and Senso also offers a specific app for iOS which replaces the Safari browser to enable comprehensive web filtering. For all other
		non-browser web apps we strongly recommend using an MDM solution that restricts apps that gain access to the internet.
• Multiple language support – the ability for the system to manage relevant languages		More than 200 languages are supported.
• 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)		In response to the increase in remote teaching and learning, Senso is entirely cloud-based and as such does not require on-premise network filtering infrastructure. This means that it can support devices whether they are on or off the school network.
• 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		Senso is a cloud-based solution which means that there is no difference in filtering quality whether a device is in school or elsewhere. If preferred, there is the option to schedule the Senso Filter Cloud to turn on once a device leaves the network or at specific times.

• Reporting mechanism – the ability to report inappropriate content for access or blocking		Senso has a section called 'Concern Reports' which is a record of all manually reported sites. We are currently working on implementing a user-driven reporting mechanism for reporting inappropriate content.
• Reports – the system offers clear historical information on the websites visited by your users		In the premium Content Filtering package, all websites visited by users are logged within Senso.

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*".[2]

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

Senso offers its existing customers a free Learning Management System (**Senso Learn**) through which school staff members, of all roles, can take specific Safeguarding courses in order to best support children in keeping safe online as well as in the classroom.

Other ways Senso can support schools with Safeguarding:

Senso Safeguard Cloud

Senso Safeguard Cloud offers cloud-based, real-time monitoring of activity on school-owned devices, designed to highlight to school staff users who may be vulnerable, a risk to themselves, a risk to others, or behaving inappropriately. Senso indicates a potential concern by raising a "violation" when a keyword, acronym or phrase types by a user matches against those found within our libraries. The violation information including a screenshot can then be viewed in the dashboard by the relevant Senso Safeguarding portal user. The screenshot will also be analysed by our AI-driven image analyser to indicate whether a student is potentially viewing harmful or inappropriate content alongside the keyword typed; this helps with prioritisation of Senso violations. Senso Safeguard Cloud integrates with CPOMS & MyConcern to support seamless reporting, and has a live dashboard to facilitate proactive and strategic online safeguarding. Users can also anonymously report a concern about themselves or someone else and include a screen capture if required.

Senso Safeguarding for Microsoft Teams App

Senso has the capability to monitor all Microsoft Teams Chat regardless of the device or location of a user. Senso Teams monitoring also analyses images alongside the text chats to identify highrisk users or behaviours. Violation information, including chat transcripts, can then be viewed in the dashboard by the relevant Senso Safeguarding portal user. All images sent within Microsoft Teams chat are also analysed by our AI driven image analyser to indicate whether a student is potentially sending harmful or inappropriate images.

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

Senso Safeguarding Assisted Monitoring Service

Senso users may also opt to benefit from our assisted monitoring service with human screening/moderation of violations, including external escalation and real-time evaluation of events by safeguarding experts. Effective triage, including phone calls for the most serious cases, means that user violations receive the appropriate level of attention.

Senso Class Cloud

Senso's classroom management software enables teachers to take control of the class and keep students focused on a task, whether the class is taking place in person or online. Teachers can actively monitor students' activity, send messages directly to devices, take control of devices, and lock users' screens for safety and attention purposes.

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 selfcertification 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	Michael Payne
Position	Director of Operations
Date	28-Apr-2023
Signature