

E-Safety Policy

Sponsorship & Review

1 Sponsor

Digital DSL

2 Reviewed

August 2024

3 Revised

December 2024

Social Media Policy

Charlton School recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online. E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility. Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures which are outlined in our behaviour policy.

1. Roles and responsibility

The School e-Safety Coordinator is Assistant Vice Principal for Safeguarding, Angela Bithell

The designated member of the governing body responsible for e-safety is Ricki Thiara

2. Communicating school policy

This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during PSHEE lessons where personal safety, responsibility, and/or development are being discussed.

3. Making use of ICT and the internet in school

The internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life,

education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school. Some of the benefits of using ICT and the internet in schools are:

For students:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking

4. Learning to evaluate internet content

With so much information available online it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiarism very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The school will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the school e-safety coordinator. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively. (Appendix 1)

5. Managing information systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by the IT technicians and network manager and virus protection software will be updated regularly.

Some safeguards that the school takes to secure our computer systems are:

- ensuring that all personal data sent over the internet or taken off site is encrypted
- making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- files held on the school network will be regularly checked for viruses
- the use of user logins and passwords to access the school network will be enforced
- portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

For more information on data protection in school please refer to our data protection policy. More information on protecting personal data can be found in section 11 of this policy.

6. Emails

The school uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication. It is also used to enhance the curriculum by:

- initiating contact and projects with other schools nationally and internationally
- providing immediate feedback on work, and requests for support where it is needed.

Staff and pupils should be aware that school email accounts should only be used for school-related matters, ie for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

6.2 School email accounts and appropriate use

Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in school. Students should be aware of the following when using email in school, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:
 - in school, pupils should only use school-approved email accounts
 - excessive social emailing will be restricted
 - pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
 - pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.
 - Pupils will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

7. Published content and the school website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects. The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office only. For information on the school policy on children's photographs on the school website please refer to section 7.2 of this policy.

7.2 Policy and guidance of safe use of children's photographs and work

Colour photographs and pupils work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school's policy on the use of photographs of children, including:

- how and when the photographs will be used
- how long parents are consenting the use of the images for
- school policy on the storage and deletion of photographs.

Using photographs of individual children.

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place. It is important that published images do not identify students or put them at risk of being identified. The school is careful to ensure that images published on the school website cannot be reused or manipulated through watermarking and browser restrictions. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission.

The school follows general rules on the use of photographs of individual children:

Parental consent must be obtained.

Consent will cover the use of images in:

- all school publications
 - on the school website
 - in newspapers as allowed by the school
 - in videos made by the school or in class for school projects.
 - through the school's social media channels
- Electronic and paper images will be stored securely.
 - Names of stored photographic files will not identify the child.
 - Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (ie a student in a swimming pool, rather than standing by the side in a swimsuit).

- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only.
- Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils. For more information on safeguarding in school please refer to our school child protection and safeguarding policy.

6.3 Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our complaints policy for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools' child protection and safeguarding policy and behaviour policy.

6.4 Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school. There are various restrictions on the use of these sites in school that apply to both students and staff. Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHEE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from

the school website with the approval of a member of staff and will be moderated by a member of staff.

- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

8. Mobile phones and personal device

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

- they can make pupils and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material
- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged, or lost
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that mobile phones are used responsibly in school. Some of these are outlined in our mobile devices policy.

9. Cyberbullying

Cyberbullying, as with any other form of peer on peer abuse, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the behaviour policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action. If an allegation of bullying does come up, the school will:

- take it seriously
- act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- record and report the incident
- provide support and reassurance to the victim
- make it clear to the 'bully' that this behaviour will not be tolerated.

If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions. If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school. Repeated bullying may result in a fixed-term exclusion.

10. Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

11. Protecting personal data

Charlton School believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision. We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the school will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect. For more information on the school's safeguards relating to data protection read the school's data protection policy.

[Appendices](#)

Appropriate Filtering for Education settings



May 2023

Filtering Provider Checklist Responses

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	Lightspeed Systems
Address	Phoenix House, Christopher Martin Road, Basildon, Essex, SS14 3EZ
Contact details	+44 (0) 20 4534 5200 / sales@lightspeedsystems.com
Filtering System	Lightspeed Filter™
Date of assessment	July 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
<ul style="list-style-type: none"> Are IWF members 		Lightspeed Systems has been a member of IWF since 2009.
<ul style="list-style-type: none"> and block access to illegal Child Abuse Images (by actively implementing the IWF URL list) 		Web pages or URLs that depict indecent images of children, advertisements for such content, or links to it are illegal and constantly tracked by IWF (Internet Watch Foundation). Lightspeed Systems immediately updates its Filter categories to match the IWF list and completely lock down access.
<ul style="list-style-type: none"> Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' 		To assist schools in complying with the Prevent Duty Guidance of the United Kingdom Counter Terrorism and Security Act 2015, Lightspeed Systems has established the violence.extremism category. This category is populated with a list of web addresses that promote extremism and/or radicalisation and is provided from The Home Office in the UK. The violence.extremism category is updated each time the Home Office supplies us with a list. Advanced reporting features allow IT administrators to easily view Internet activity across the whole school- or drill down to individual user activity. Also, email alerts can be set up so suspicious search activity notifies designated staff.
<ul style="list-style-type: none"> Confirm that filters for illegal content cannot be disabled by the school 		All websites categorised as illegal in Lightspeed's extensive, constantly updated URL database are placed in sealed categories that cannot be allowed by any IT admin or member of staff in a school or organisation.

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.		When a user attempts to search for anything, a list of keywords is referenced. If the search includes any discriminatory or offensive words on the list, access will be blocked. Our importable flagged keyword list contains hundreds of entries, and admins can customise the list with their own keywords that best match their communities.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		We have specific categories for blocking access to <i>drugs</i> and <i>alcohol</i> .
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Our <i>violence.extremism</i> category contains all of the latest URLs from the Home Office that promote terrorism, terrorist ideologies, violence or intolerance—as well as URLs added by the worldwide education community.
Gambling	Enables gambling		Lightspeed Filter's <i>gambling</i> category blocks all websites related to gambling, casinos, betting, lottery and sweepstakes.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Malware and other malicious content is blocked before it reaches the network. Our database categorises sites with demonstrated or potential security risks into several security categories, and for extra safety, all unknown URLs can be blocked.
Pornography	displays sexual acts or explicit images		Naturally all pornographic material in the <i>porn</i> category is blocked. In addition, potentially illegal pornographic material is locked as well as a second category <i>porn.illicit</i> containing potentially illegal pornographic material. This is a sealed category and cannot be unblocked.
Piracy and copyright theft	includes illegal provision of copyrighted material		Our category <i>forums.p2p</i> blocks access to all peer-to-peer and file-sharing sites that would

			enable plagiarism or sharing copyrighted material.
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		To prevent any students from looking at websites that promote or display self-harm, again the blocked-search key words is referenced; and a number of different categories can be controlled such as <i>forums</i> and <i>adult</i> . Our safeguarding solution Lightspeed Alert™ built into the uses advanced AI and a 24/7 safety specialist team to notify administrators instantly when a student types anything relating to self-harm online. Alert works across all productivity and education apps, files, chat including Microsoft Teams and Google Workspace and provides schools with a timeline of the event including screenshots and activity logs.
Violence	Displays or promotes the use of physical force intended to hurt or kill		Our <i>violence</i> category contains all sites that promote the use of physical force intended to harm or kill. Lightspeed Alert also notifies schools and admins when students type anything related to violence.

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

Lightspeed Systems uses our online database that leverages AI, machine learning, and the infinite cloud for the most accurate and comprehensive categorisation of the Web. Schools have the ability to restrict access to certain categories or to unknown URLs.

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 retain data for as long as necessary to fulfil the purposes for which it was collected for. Following termination or deactivation of a School account, Lightspeed Systems may retain profile information and content for a commercially reasonable time for backup, archival, or audit purposes, but all Student Data associated with the School will be deleted in accordance with Lightspeed Systems Data Deletion policy, or in accordance with active DPA, DSA or SLA. We may maintain anonymised or aggregated data, including usage data, for analytics purposes.

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

Customers are able to customise the filter to meet their local needs including allowing or blocking categorise, domains, URLs and IPs. Additionally, customers are able to configure the filter to allow normally blocked site for a period of time. Finally, as an education only based company our database is tuned for education by education via our share option where customers can share category changes with us.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
<ul style="list-style-type: none"> Context appropriate differentiated filtering, based on age, vulnerability and risk of harm – also includes the ability to vary filtering strength appropriate for staff 		<p>Lightspeed Filter has been designed specifically for education. It can be fully customised to perfectly match your organisational structure-tailoring policies based for different year groups, ability, location or for members of staff.</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>Lightspeed’s patent-pending Smart Agents filter any device, any app, any browser; and provide easy SSL decryption without proxies, PACs, or certificate hassles. Our extensive database of URL’s is constantly being updated with the latest VPN’s and filter bypassing tools and keeping them blocked.</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. 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 		<p>Tiered administration across our products allows different levels of control to be permitted to different schools and users. Designated staff can add and edit keyword lists and create local allow and block lists. YouTube access can be managed by category, channel, and video. Using Lightspeed Classroom Management™, teachers can allow or block URLs to expand or constrict access with oversight.</p>

<ul style="list-style-type: none"> 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. 		<p>Lightspeed Filter utilises a database system that dynamically scans page content to ensure that the page is correctly categorised.</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>There are more than a billion sites on the web, and thousands are added each hour. Your web filter needs to know them all.</p> <p>The adaptive AI database of Lightspeed Systems leverages AI, machine learning and the infinite cloud for the most accurate and comprehensive categorisation of the Web.</p> <p>This means you save time not having to re-categorise, and you can count on students staying safe without over blocking.</p>
<ul style="list-style-type: none"> Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard 		<p>Lightspeed Filter allows tiered levels of control based on user’s roles in the organisation, as well as centralised policies that work across entire schools, local authorities or trusts.</p>
<ul style="list-style-type: none"> Identification - the filtering system should have the ability to identify users 		<p>Lightspeed Filter can integrate with authorisation sources to gather user credentials, be configured for a captive portal or use local accounts.</p> <p>Lightspeed identifies users through a range of different methods including a web portal, agent (application) identification, and RADIUS integration.</p>
<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 		<p>All traffic that passes through a school or college network can be intercepted, including content via mobile and app technologies. If</p>

<p>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</p>		<p>inappropriate apps are the issue, Lightspeed Mobile Device Management™, utilises app management to control device apps and restrictions.</p>
<ul style="list-style-type: none"> Multiple language support – the ability for the system to manage relevant languages 		<p>Our <i>world</i> categories contain websites from multiple countries that can be filtered accordingly. Flagged keywords can be added in any language to flag suspicious or concerning user activity. Further, we can enforce Google safe search, which has Google's own rules in multiple languages.</p>
<ul style="list-style-type: none"> 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) 		<p>Our patent pending Smart Agents sit on every device and are able to monitor all traffic and provide easy SSL decryption without proxies, PACs, or certificate hassles. For BYOD deployments, a virtual appliance easily installed on your network catches every bit of traffic the Smart Agents can't.</p>
<ul style="list-style-type: none"> 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 		<p>Lightspeed Filter uses patented Smart Agents that sit on every device to give schools the same level of filtering on any device and any OS remotely. Schools can also enable "after school rules" and time or location-based policies to these devices to ease restrictions accordingly</p>
<ul style="list-style-type: none"> Reporting mechanism – the ability to report inappropriate content for access or blocking 		<p>We provide an extensive list of reporting and options to create customised and easily shareable reports.</p>
<ul style="list-style-type: none"> Reports – the system offers clear historical information on the websites users have accessed or attempted to access 		<p>Admins have immediate access to pre-installed web activity reports that may be customised by date range, school, and group.</p>
<ul style="list-style-type: none"> Safe Search – the ability to enforce 'safe search' when using search engines 		<p>We allow schools to force Safe Search for the entire school or individual groups.</p>

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

Digital Driver’s License for Digital Citizenship:

Website: <http://iDriveDigital.com>

Store: <https://itunes.apple.com/us/app/idrivedigital/id550609295?mt=8>

Google Play:

<https://chrome.google.com/webstore/detail/ddl/jpohacgnbefbjlgfdpekngggppkolgdn?hl=en>

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	Brian Thomas
Position	President & CEO
Date	29 TH July 2023
Signature	

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

Appropriate Filtering for Education settings



April 2023

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” 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
<ul style="list-style-type: none"> Are IWF members 		Senso is a member of the IWF and actively communicates with them.
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role 		Senso Content Filtering can: <ul style="list-style-type: none"> - 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.

<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>Senso blocks access to torrent repositories, proxy anonymisers, and peer-to-peer file-sharing sites to help prevent circumvention.</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>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.</p>
<ul style="list-style-type: none"> ● 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 		<p>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.</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>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.</p>
<ul style="list-style-type: none"> ● Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard 		<p>Senso Content Filtering is scalable and flexible to support multi-site management from the top level right down to individual user-specific filtering policies.</p>
<ul style="list-style-type: none"> ● Identification - the filtering system should have the ability to identify users 		<p>Users are identified when they log on to the device.</p>
<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>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</p>

		non-browser web apps we strongly recommend using an MDM solution that restricts apps that gain access to the internet.
<ul style="list-style-type: none"> Multiple language support – the ability for the system to manage relevant languages 		More than 200 languages are supported.
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> 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”*.¹

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

Senso Safeguarding Assisted Monitoring Service

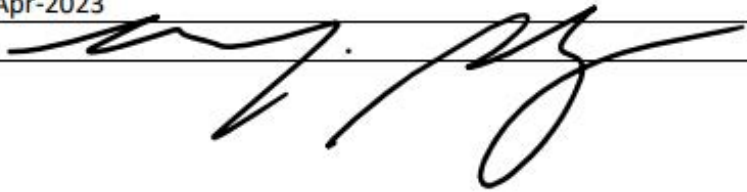
Senso users may also opt to benefit from our assisted monitoring service with human screening/moderation of violations, including external escalation and real-time evaluation of events by safeguarding experts. Effective triage, including phone calls for the most serious cases, means that user violations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

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

Telford & Wrekin IDT Managed Services



Education & Skills
Funding Agency

Academy trust guide to cyber crime and cyber security

Telford and Wrekin IDT Services Response October 2022



Services
for schools



www.twccommercial.co.uk

servicesforschools@telford.gov.uk

01952 380522

Contact us to discuss your requirements

Introduction

- Kirsty King - IDT Service Delivery Manager
- Presentation content provided by :
 Andy Carpendale – IDT Security Specialist

ESFA Checklist

Cyber crime: what can trusts do?

- To comply with the requirements of the Academies Financial Handbook (paragraph 4.8.1) and address the risk of fraud, theft and/or irregularity, trusts should as a minimum:
- use firewalls, antivirus software and strong passwords
- routinely back up data and restrict devices that are used to access data
- train staff to ensure that they:
 - check the sender of an email is genuine before, for example, sending payment, data or passwords
 - make direct contact with the sender (without using the reply function) where the email requests a payment
 - understand the risks of using public wifi
 - understand the risks of not following payment checks and measures

ESFA Checklist

Cyber crime: what do Telford and Wrekin IDT Services provide:

- Boundary firewall protection with internet filtering and proxy technology that protects machines from direct connectivity to the Internet.
- Antivirus protection is installed on all machines and updates every 2 hours. Any portable media is scanned when attached
- Deploy fine grained password policies which schools can use to set strong passwords, we also use a user creation toolkit so the password reset process can be delegated to the school.
- A backup solution that is hosted in the IDT Services datacentre. Backups run every morning and evening, with the SIMS database every 4 hours. Retention period is currently 90 days.
- As part of our investment in office365, multifactor authentication is available to provide extra security around logins into the office365 service.

ESFA Checklist

Cyber crime: what do Telford and Wrekin IDT Services provide:

- Regular email reminders about SPAM and Phishing Attacks and what you should do guidance.
- We can provide specific training on request.
 - Schools and Trusts procure Audit and Scrutiny advise through a number of different suppliers and we can support this.

ESFA Checklist – 5 Strategic Questions

1. Information Held

Does the trust have a clear and common understanding of the range of information assets it holds and those that are critical to the business?

We are able to help assist with audits.

ESFA Checklist – 5 Strategic Questions

2. Threats

Does the trust have a clear understanding of cyber threats and vulnerabilities?

Are you aware? Risks of sharing data over personal accounts, storage of any data, password security?

National Cyber Security Centre – Board Toolkit

Resources designed to encourage essential cyber security discussions between the Board and their technical experts.

<https://www.ncsc.gov.uk/collection/board-toolkit>

ESFA Checklist – 5 Strategic Questions

3. Risk management

Is the trust proactively managing cyber risks as an integrated facet of broader risk management including scrutiny of security policies, technical activity, user education and testing and monitoring regimes against an agreed risk appetite?

Automated internal vulnerability assessments are completed on a weekly basis and externally on a bi-monthly basis by an approved 3rd party.

Logging of privileged user activity, permission changes and access.

User awareness training around security themes is available on request

ESFA Checklist – 5 Strategic Questions

4. Aspects of risk

Does the trust have a balanced approach to managing cyber risk that considers people (culture, behaviours and skills), process, technology and governance to ensure a flexible and resilient cyber security response?

We maintain an IDT Risk Register which feeds into the Council's corporate risk register where the risk score is deemed as high.

Solutions and services will be risk managed as part of the project delivery mechanism or as part of the procurement process.

We report to a quarterly Governance Board chaired by Head Teachers on performance and any Cyber Security concerns.

ESFA Checklist – 5 Strategic Questions

5. Governance oversight

Does the trust have sound governance processes in place to ensure that actions to mitigate threats and maximise opportunities in the cyber environment are effective?

Report to a quarterly Governance Board chaired by Head Teachers on performance and any Cyber Security concerns.

Operate a change management board weekly.

Representation on the Council Security Group.

ESFA Checklist – 10 Steps

1. Home and mobile working

- A secure baseline build which can include encryption is applied to all equipment, delivered as part of our deployment process and this is the same deployment method for monthly security patches.
- We provide data in transit security as part of the remote access solution, Schools can also request bit locker for devices for data at rest protection as part of our bit locker encryption offering. Email encryption is also available.

ESFA Checklist – 10 Steps

2. User education and awareness

- User awareness training around security themes is available on request.
- Regular email reminders about SPAM and Phishing Attacks and what you should do.
- Issues and incidents can be reported via the IDT Self Service or if this is a priority 1 incident via Telephone (where appropriate)

ESFA Checklist – 10 Steps

3. Incident management

- We use ITIL Incident and Problem Management processes, in a major incident we will invoke an Emergency Response Team which will link into the council resilience team as appropriate.
- Disaster recovery capability through backup solution.
- IDT Services will work with or report to Schools SMT, Council Audit, internal Human Resources departments and law enforcement when required to do so.

ESFA Checklist – 10 Steps

4. Information risk management regime

- Update an IDT Risk Register which feeds into the Council's corporate risk register where the risk score is deemed as high.
- We will report risks to Head Teachers within schools and to the Governance Board.
- IDT have membership of the National Cyber Security Centre's Cyber Information Sharing partnership to discuss and to gather intelligence relating to cyber security threats.

ESFA Checklist – 10 Steps

5. Managing user privileges

- Provide a user management toolkit for key staff within school and reporting is also available on request.
- Privileged accounts are monitored and restricted to permitted personnel only.
- Monitor and control access to log data, IDT use log analytical technology to monitor for unusual behaviour.

ESFA Checklist – 10 Steps

6. Removable media controls

- Provide an endpoint/device antivirus solution to enable staff to scan removable media.

ESFA Checklist – 10 Steps

7. Monitoring

- We have monitoring solutions and capabilities in place across our systems and networks. Ranging from reliability monitoring to threat monitoring allowing the ability to detect unusual activity.
- We use a product called Senso to enable schools to monitor usage. Designed with the UK Government Prevent duty, UK Safer Internet Centre, the UK Department for Education's Keeping Children Safe in Education (KCSiE) guidance and with keyword and URL lists from the Internet Watch Foundation(IWF) aids schools in fulfilling their legal duty of care around online safety and safeguarding.

ESFA Checklist – 10 Steps

8. Secure configuration

- Can assist with completion of a system inventory which will list the information on machines that you have joined to your network.
- Provide a secure defined baseline build which is delivered as part of a deployment process, this is the same deployment method for monthly security patches.
- Complete monthly patching in line with the IDT Services Patch Management Policy.

ESFA Checklist – 10 Steps

9. Malware protection

- Provide antivirus and anti-malware protection on endpoints/devices, email and internet filtering, with a combination of on access and scheduled scanning in place.
- Restrictions are in place for staff and students to prevent unauthorised software installations.

ESFA Checklist – 10 Steps

10. Network security

- Manage the network perimeter including boundary or client side Firewalls.
- We manage and control access to our own datacentres, IDT can assist in reporting on high risk assets on request.
- Complete automated internal vulnerability assessments on a weekly basis and external testing is completed on a bi-monthly basis by an approved 3rd party.

Telford & Wrekin IDT Managed Services



Education & Skills
Funding Agency

Keeping Children Safe in Education Filtering and Monitoring

Telford and Wrekin IDT Services Response October 2022



www.twccommercial.co.uk

servicesforschools@telford.gov.uk

01952 380522

Services
for schools

Contact us to discuss your requirements

Filtering and Monitoring

- Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors 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.
- As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness

How do IDT meet this requirement?





- Internet Filtering Provision: Smoothwall

smoothwall[®]

– This blocks access to any of the material listed below

- Using the DfE recommended testing site by SWGfL here are the results:-

Results Overview

			
Child Sexual Abuse Content	Terrorism Content	Adult Content	Offensive Language

Filtering Provider
Smoothwall

Network
TELFORDWREKINCOUNCILAS

Reputation
Excellent

How do IDT meet this requirement?

Child Sexual Abuse Content



Description

Tests whether you are blocking websites on the IWF Child Abuse Content URL list.

Results & Recommendations

It appears that your filtering solution includes the IWF URL Filter list, blocking access to Child Sexual Abuse content online

Terrorism Content



Description

Tests whether you are blocking websites on the Counter-Terrorism Internet Referral Unit list (CTIRU).

Results & Recommendations

It appears that your filtering solution includes the Counter-Terrorism Internet Referral Unit (CTIRU) URL filter list, blocking access to unlawful terrorist content online

Adult Content



Description

Test whether your Internet filter blocks access to pornography websites

Results & Recommendations

It appears that your filtering solution includes blocking for online pornography

Offensive Language



Description




Accesses a page containing offensive language to test if your filtering software blocks it

Results & Recommendations

It appears that your filtering solution includes blocking for offensive language





UK Safer Internet Checklist

Illegal Online Content

Aspect	Rating	Explanation
Are IWF members		Yes, Smoothwall is a member of the Internet Watch Foundation and implements the IWF CAIC list
and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Smoothwall implements the IWF CAIC list of domains and URLs. Smoothwall Filter also uses a number of search terms and phrases provided by IWF and their members. We perform self certification tests daily to ensure that IWF content is always blocked through a Smoothwall Filter
Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Smoothwall Filter implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office






UK Safer Internet Checklist

Inappropriate Online Content

Aspect	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 'Intolerance' category covers any sites which promote racial hatred, homophobia or persecution of minorities. Sites which advocate violence against these groups are also covered by the Violence category.
Drugs / Substance abuse	Displays or promotes the illegal use of drugs or substances		The Drugs category covers the sale, manufacture, promotion or use of recreational drugs as well as abuse of prescription drugs. Sites which provide resources which aim to help those suffering from substance abuse are covered by the 'Medical Information' category. Sites which discuss Alcohol or Tobacco are covered by the 'Alcohol and Tobacco' category.
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance		The 'Terrorism' category contains the 'police assessed list of unlawful terrorist content'. Smoothwall also provides both a 'Violence' category which covers violence against both animals or people; An 'Intolerance' category (covered further above) and a 'Gore' category which covers any sites which describe or display gory images and video.
Malware / Hacking	Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		As well as providing a level of protection against externally created malware, Smoothwall Filter provides a Hacking category which includes sites such as "how to" on hacking, and sites encouraging malicious computer use. Filter bypass tools are covered separately in a comprehensive "web proxies" category, which uses a combination of domain lists and dynamic content analysis.

UK Safer Internet Checklist

Inappropriate Online Content

Aspect	Explanatory notes – Content that:	Rating	Explanation
Piracy and copyright theft	Includes illegal provision of copyrighted material		The 'Piracy and Copyright Infringement' category contains sites which illegally provide copyright material or provide peer-to-peer software.
Self Harm	Promotes or displays deliberate self harm (including suicide and eating disorders)		The 'Self Harm' category contains sites relating to self-harm ,suicide and eating disorders. The category excludes sites which aim to provide medical or charitable assistance which are categorised as 'Medical Information' or 'Charity and Non-Profit' respectively
Violence	Displays or promotes the use of physical force intended to hurt or kill		The 'Violence' category contains sites which advocate violence against people and animals. We also provide a 'Gore' category which contains images and video of gory content
Pornography	Display ssexual acts or explicit images		The 'Pornography' category contains sites containing pornographic images, videos and text. Sites which contain mild nudity for purposes other than sexual arousal are covered by the 'Non-Pornographic Nudity' category. The 'Pornography' category uses both a list of domains/URLs as well as dynamic content rules which ensure new, previously unseen sites can be identified on the fly.
Multiple language support – the ability for the system to manage relevant languages			Smoothwall's combined blocklist include words in a wide variety of languages, focussed on those spoken in UK and US schools. This includes Polish and Spanish as well as "non latin" such as Urdu and Russian.

How to IDT meet this requirement?




- Classroom Monitoring Provision: Senso



- More than 99% active web coverage and accuracy
Web traffic from 600+ million end users globally. Over 200 languages supported Daily and real-time updates. Senso's filter cloud 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









UK Safer Internet Checklist

Illegal Online Content

Aspect	Rating	Explanation
Are IWF members		Senso® is a member of the IWF and actively communicate with them.
and block access to illegal Child Abuse Images(by actively implementing the IWF URL list)		IWF Lists are provided 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

UK Safer Internet Checklist

Inappropriate Online Content

Aspect	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		Discrimination Category is one of 500 + unique content categories, 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
Drugs / Substance abuse	Displays or promotes the illegal use of drugs or substances		Several categories combine to cover Drugs & Substance Abuse Categories as above
Extremism	Promotes terrorism and terrorist ideologies, violence or intolerance		Extremism category as above plus 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		Yes – covered within Malicious Internet Activity Category
Pornography	Display ssexual acts or explicit images		Adult Content Category included as above
Piracy and copyright theft	Includes illegal provision of copyrighted material		Covered within Criminal Activity / Piracy Category
Self Harm	Promotes or displays deliberate self harm (including suicide and eating disorders)		Self Harm Category included as above
Violence	Displays or promotes the use of physical force intended to hurt or kill		Weapons / Violence category included as above

How to IDT meet this requirement?

- Senso Safeguard Cloud :
- Cloud based, real time monitoring of activity on school owned devices, designed to highlight to school staff users who may be vulnerable or at risk to themselves, at risk to others or behaving inappropriately. Senso indicates a potential concern by raising a “violation” when a keyword, acronym or phrase typed, 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 analysis to indicate whether a student is potentially viewing harmful or inappropriate content alongside the keyword typed. This helps with prioritisation of Senso violations.
- Integrates with CPOMS & Myconcern - If your school would like this integration please log a call on the IDT portal or speak to your IDT Gold Technician.

