

Garswood Primary School

- Filtering and Monitoring Policy

At Garswood our Internet filtering and monitoring is controlled by a company called **'Smoothwall'** through St Helens Council.



Keeping Children Safe in Education:

Safeguarding in Schools

Schools and colleges should provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It's important that the right people are working together and using their professional expertise to make informed decisions.

	Person(s) responsible	
a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met	Les Moon (SLT) Ian Green (Gov)	Pam Potter (DSL) Lee Pearson (ISP)
the roles and responsibilities of staff and third parties, for example, external service providers	Pam Potter (DSL and Head teacher)	

Keeping children safe in education makes it a statutory requirement that schools safeguard children and young people from potentially harmful and inappropriate online material. The guidance states that whilst the breadth of issues classified within online safety is considerable and ever-evolving, they can be categorised into four areas of risk; **content, contact, conduct and commerce.**

SLT responsibilities:

In relation to Computing Systems	In relation to School Staff
<ul style="list-style-type: none"> • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports 	<ul style="list-style-type: none"> • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns

DSL and ISP responsibilities:

Day to day management of filtering and monitoring systems requires the specialist knowledge of both our safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers at St Helens Council to meet the needs of Garswood.

The DSL should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

	DSL	ISP	SLT
filtering and monitoring reports	✓		
safeguarding concerns	✓		
checks to filtering and monitoring systems	✓		
maintaining filtering and monitoring systems		✓	
providing filtering and monitoring reports		✓	
completing actions following concerns or checks to systems		✓	
procure systems	✓	✓	✓
identify risk	✓	✓	✓
carry out reviews	✓	✓	✓
carry out checks	✓	✓	✓

Filtering and Monitoring is highlighted within the KCSIE document, emphasising the following areas below. This policy on Filtering and Monitoring at Garswood should highlight how these areas are covered within our school.

- 🌐 **Paragraph 103, p.28:** DSLs now have a responsibility for “understanding the filtering and monitoring systems and processes in place” as part of their remit.
- 🌐 **Paragraph 124, p.32:** Governing bodies should ensure that all staff undergo safeguarding and child protection training. It should give them “an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring” (paragraph 124, p.32).
- 🌐 **Paragraph 138, p.36:** A school’s child protection policy should include how it approaches ‘appropriate filtering and monitoring on school devices and school networks.’
- 🌐 **Paragraph 142, p.37:** “Schools and colleges should consider meeting the DfE’s new Filtering and Monitoring Standards and Cyber Security Standards (paragraph 144, p.38)

🌐 Technical requirements to meet the standard

A review of filtering and monitoring is carried out annually to identify your current provision, any gaps, and the specific needs of your pupils and staff.

The review results below are from **January 2025**

	DSL	ISP	SLT
Do I have an understanding of.....?			
🌐 any outside safeguarding influences, such as county lines	✓	✓	✓
🌐 what your filtering system currently blocks or allows and why	✓	✓	✓
🌐 the risk profile of your pupils, including age, with SEND and EAL	✓	✓	✓
🌐 any relevant safeguarding reports	✓	✓	✓
🌐 the digital resilience of your pupils	✓	✓	✓
🌐 teaching requirements, e.g., your RHSE and PSHE curriculum	✓	✓	✓
🌐 the specific use of your chosen technologies, including BYOD	✓	✓	✓
🌐 what related safeguarding or technology policies are in place	✓	✓	✓
🌐 checks that are currently in place and how actions are handled	✓	✓	✓

	DSL	ISP	SLT
Does my filtering and monitoring review inform.....?			
related safeguarding or technology policies and procedures	✓	✓	✓
roles and responsibilities	✓	✓	✓
training of staff	✓	✓	✓
curriculum and learning opportunities	✓	✓	✓
procurement decisions	✓	✓	✓
how often and what is checked	✓	✓	✓
monitoring strategies	✓	✓	✓

Reporting of Incidents:

All staff are aware of reporting mechanisms for safeguarding and technical concerns. They should report to the DSL and record on CPOMS if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

Monitoring allows us as staff at Garswood to review user activity on school devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing us to take prompt action recording the outcome.

Garswood's monitoring strategy is informed by the filtering and monitoring review. A variety of monitoring strategies are required to minimise safeguarding risks on internet connected devices:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

Smoothwall Visions and Values:

Online safety for people at school or at work lies at the heart of our culture and is the embodiment of our values in action.

Smoothwall Filter

A key challenge for schools is to ensure adherence to their acceptable usage policy without restricting access to key functions and services. Preventing over-blocking and unreasonable restrictions is critical.















Smoothwall's web filtering is favoured by the public sector organisations because of its real-time content-aware analysis. It scans the copy, content and context of every page for unwanted material and has 120 filtering categories which can be used to tailor the web browsing experience of all audiences to ensure that harmful content is out of reach.

Combined with a powerful reporting suite, social media controls and BYOD functionality, Smoothwall Filter allows you to review and control what employees see and do online. Our Anti-malware also provides protection against malware and ransomware threats.

Garswood uses the **'Cloud' deployment option** through St Helens local authority which is monitored at St Helens Town Hall by expert technicians. Reports are generated immediately and emailed to the school DSL, Head teacher and Computing lead.

Key Features:

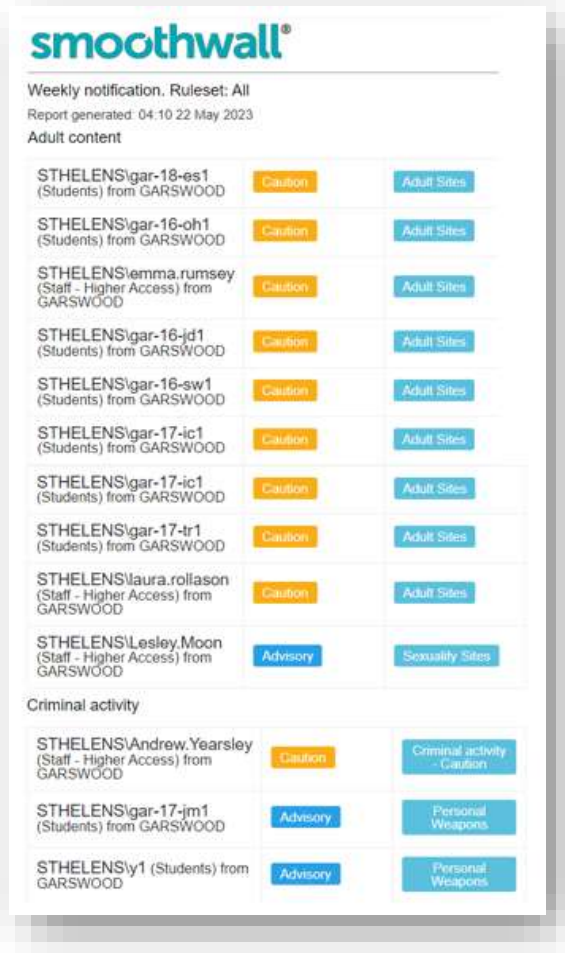
 <p>Real-Time Dynamic Content Analysis</p> <p>Categorises new and existing web content appropriately in real-time by analysing the content, context and construction of each page.</p>	 <p>Safeguarding</p> <p>The safeguarding reporting suite notifies you of any safeguarding risk against seven category rule sets including radicalisation, suicide and self harm.</p>	 <p>Social Media Controls</p> <p>Flexible tools allows read-only access and the ability to remove inappropriate content across social media sites.</p>
 <p>BYOD</p> <p>Offer public WiFi filtering and filter guest mobile devices securely on your network across all platform.</p>	 <p>Multi-OS Support</p> <p>Available on Chrome OS, Windows, macOS, and iOS devices.</p>	 <p>HTTPS Filtering</p> <p>Filter Secure Socket Layer (SSL) traffic, including secure anonymous proxies.</p>
 <p>Who, What, Where, When</p> <p>Build policies based on user group, content category, time, location IP, subnet and hostname for mobile devices and laptops.</p>	 <p>Easy Management</p> <p>Intelligently manage and allocate bandwidth to minimise the impact of media and file sharing without the need in bulky block services.</p>	 <p>Granular Reports</p> <p>You can generate reports to view the activity of individuals and groups, and enable automatic reports.</p>
 <p>Anonymous Proxy Blocking</p> <p>Prevent circumvention of your Acceptable Use Policy.</p>	 <p>Gateway Anti-Malware</p> <p>Ensure your organisation is secured against malware and ransomware threats.</p>	 <p>Layer 7 Application Control</p> <p>Identify and stop applications that you don't want on your network and prioritise those that you do.</p>

Smoothwall Firewall

Smoothwall's Firewall solution has all the features and benefits of the Smoothwall Filter. It can be purchased independently or combined to offer a unified threat management solution. As KCSIE states it is crucial to ensure the highest levels of safety are in place for our children and therefore we have both options available at our school.

Smoothwall's Firewall combines Layer 7 application control with perimeter firewall and stateful packet inspection to provide Next-Generation firewall functionality. Smoothwall Firewall also features anti-malware protection, HTTPS inspection, anonymous proxy detection & blocking, and intrusion detection & prevention, to provide you with a complete all-in-one protection package designed with your organisation's security needs in mind.

All built into one appliance, you can provide cost-effective protection for your network and shield against all web and non-web borne threats.



Weekly notification. Ruleset: All
Report generated: 04:10 22 May 2023
Adult content

STHELENS\gar-18-es1 (Students) from GARSWOOD	Caution	Adult Sites
STHELENS\gar-16-oh1 (Students) from GARSWOOD	Caution	Adult Sites
STHELENS\emma.rumsey (Staff - Higher Access) from GARSWOOD	Caution	Adult Sites
STHELENS\gar-16-ld1 (Students) from GARSWOOD	Caution	Adult Sites
STHELENS\gar-16-sw1 (Students) from GARSWOOD	Caution	Adult Sites
STHELENS\gar-17-ic1 (Students) from GARSWOOD	Caution	Adult Sites
STHELENS\gar-17-ic1 (Students) from GARSWOOD	Caution	Adult Sites
STHELENS\gar-17-tr1 (Students) from GARSWOOD	Caution	Adult Sites
STHELENS\laura.rollason (Staff - Higher Access) from GARSWOOD	Caution	Adult Sites
STHELENS\Lesley.Moon (Staff - Higher Access) from GARSWOOD	Advisory	Sexuality Sites

Criminal activity

STHELENS\Andrew.Yearsley (Staff - Higher Access) from GARSWOOD	Caution	Criminal activity - Caution
STHELENS\gar-17-im1 (Students) from GARSWOOD	Advisory	Personal Weapons
STHELENS\y1 (Students) from GARSWOOD	Advisory	Personal Weapons

Key Features:

 <p>Next Generation Firewall Perimeter firewall and internal segmentation firewall to protect networks against all web and non-web threats.</p>	 <p>Layer 7 Application Control Identify and stop applications that you don't want on your network and prioritise those that you do.</p>	 <p>Intrusion Detection and Prevention Monitor, report on and react to any malicious attacks on your systems.</p>
 <p>Bandwidth Management Limit bandwidth use by content type, user, time and location, and web proxy cache.</p>	 <p>VPN Supports both Site-to-Site (IPsec) VPNs and Remote Users (SSL and L2TP).</p>	 <p>Link and Load Balancing Support for multiple WAN connections.</p>
 <p>Directory Server Integration Microsoft Active Directory, Open Directory, eDirectory and more.</p>	 <p>Gateway Anti-Malware Check signatures of malicious content at the gateway and protect against known and zero-day threats.</p>	 <p>Source Natting Ensure traffic going out over multiple IPs is correctly routed.</p>

Smoothwall Monitor










Helping public organisations to detect online risks before they become real-life incidents. Smoothwall Monitor is a real-time, digital monitoring solution that flags incidents as they happen. Monitoring both keystrokes and screen views, designated individuals are informed, through a variety of means, when users try to view or type harmful content.

In our self-service option can identify content that may indicate risk to an employee such as violence, suicide, radicalisation, criminal activity, or an inappropriate use of company resources.

Alternatively, in our managed service option, a team of human moderators will identify risks on your behalf, alerting you by email for low level risk or by phone for higher risks needing your immediate attention.

Early identification of a risk means early intervention and improved outcomes for the individual and their organisation. St Helens has opted for the managed service option so we can link specific log ins to associated incidents as quick as possible.

Key Features:

 <p>Cloud-Based</p> <p>Easy to install technology with remote set-up options and updates.</p>	 <p>Auto Pre-Grading</p> <p>Reduces false positives and improves administrative collaboration to minimise oversight.</p>	 <p>Accessible</p> <p>Software can be securely accessed anywhere by administrators on any device.</p>
 <p>Intuitive Interface</p> <p>Incidents are displayed using highly visual heat maps and graphs allowing you to quickly review performance and view individual alerts.</p>	 <p>Real-Time Monitoring</p> <p>Keystrokes and on-screen content are auto-moderated and pre-graded in real-time allowing you to promptly identify and address issues of concern as they occur.</p>	 <p>Customisable</p> <p>Flexible management to align with your school's digital safeguarding plans. User groups and specific terms can be easily modified to meet data security requirements.</p>
 <p>Easy Reports and Alerts</p> <p>Automatic reporting can make data retrieval fast and readily available. Alerts can be sent in real-time and can be varied by risk level.</p>	 <p>Managed Service (formerly Visigo)</p> <p>A highly-trained team monitors your alerts and notifies you of risks appropriate to their grade.</p>	 <p>Self-Service (formerly RADAR)</p> <p>Manage your alerts in-house with our easy to use interface.</p>

Working in Schools:

7 imperatives every Computing lead and DSL needs to consider when choosing a web filter for their school.

“At Smoothwall we support councils to meet their duty to provide web security for their corporate environments, education customers and public access schemes.”

As market leaders in the UK public sector, Smoothwall pride themselves on their ability to continually meet the needs of this complex and ever-changing school setting, by engaging in direct strategic relationships with customers and providing unrivalled support from dedicated offices based in the UK.



Market-leading dynamic content filtering currently covers more than 90 UK council networks and helps to secure children in more than 10,000 UK schools.

Safeguarding in Education:

“Whilst we didn’t need support during the installation because there wasn’t a single issue, as the project grew Smoothwall’s support became a trusted friend.”

Who, what, where and when:

Primary Schools have complex needs when it comes to internet access and digital safeguarding. It's typical to have students that span a broad range of ages, nationalities, and who have a

diverse mix of device types. Also, students with 24/7 Wi-Fi access from their own devices. It's a fine balance between giving students the freedom to learn as part of a world class education and the duty of care to protect their wellbeing. The web filtering policy controls within Smoothwall Filter help schools achieve these aims in an intuitive, flexible and powerful policy system.

	Who	What	Where	When	Action	Enabled
1	Everyone	Everything	Everywhere	Always	Default Blockpage	<input checked="" type="checkbox"/>
2	Students	Online Shopping	Everywhere	Always	Default Blockpage	<input checked="" type="checkbox"/>

Who	Garswood implements filtering based on age group, with content restricted more heavily for younger pupils. Staff may still have filtering applied, but with a much less restrictive policy. These groups come from existing authentication systems such as Microsoft Active Directory. It is also possible to apply filtering policies to individual users if required.
What	Smoothwall use a dynamic content analysis engine to analyse 200+ categories which gives the ability to apply policies using constantly updated definitions. St Helens Council can also create their own categories to apply rules, such as walled gardens. These may be used during exams, prep or can be used to limit users to a specific list of websites only.
Where	Our school network although small is linked to all St Helens schools. It covers all classrooms, dining areas, sports facilities council buildings. The ability to apply differing filtering policies based on the physical location of a user gives powerful controls to schools, such as allowing access to games only from specific places.
When	The need to differentiate filtering policies depending on time of day may still be required. Break times, after-school activities and clubs may require different rules to the main school day. Quota controls is not currently used in this way but can be used to implement digital wellbeing controls – such as limiting students to 30 minutes Minecraft media per day, and only between certain hours and from specific locations.

AI in schools:

The most important question to ask is where does your filter apply these AI techniques? It's commonly in one of two areas:






- 1.** In line with the web filtering in real-time Real-time filtering is either baked into a network appliance, or is part of a filtering client. There are occasional updates to the rules database, but generally, the filter makes all decisions locally.
- 2.** Out-of-band offline processing With out-of-band intelligence, uncategorised URLs are fed back to the filter vendor, and the site is then visited by an automated web crawler or "spider". The results are then passed through the intelligent system, and a categorisation attached to the URL. The categorisation makes it back to the point of filtering in regular URL list updates.

	Inline	Out of Band
Speed of reaction	Instant - Any filtering decision is applied straight away, leaving no opportunity for harmful content to get by.	Slow - Unknown content is queued waiting for the offline process to occur. Filtering is then caught up at the next regular update.
Effectiveness: Real-time content	Excellent - Real-time or rapidly changing content is reassessed each time, so a correct decision is made against up to date data.	Poor - Generally the categorisation of a site is either permanently fixed, or fixed for months. leaving sites with changing content open to misclassification.
Effectiveness: Context	Weak - Inline filters only see one page at a time and can't make decisions based on what's linked to.	Strong - An out-of-band web filter can check a lot of context around the page
Effectiveness: Logged-in content	Excellent - As these filters work on the data the user sees, even content behind a login such as a forum or social media will get scanned.	Ineffective - The out of band filter sees only the login page, which rarely provides any actionable content.
Additional latency	Low - Usually adding intelligence will add latency to each request. Properly designed systems will limit this so it isn't noticed by the user.	Zero - As all intelligence is out of band, there's no additional latency.

Regulation of Investigatory Powers act (RIPA)

RIPA gives the Police as well as other government bodies such as The Gambling Commission and The Food Standards Agency – a way to access communication data. For schools, this means that we may need to provide information about a user's access to a particular site. This is often in conjunction with PREVENT and tackling extremism but it can be for other purposes too.

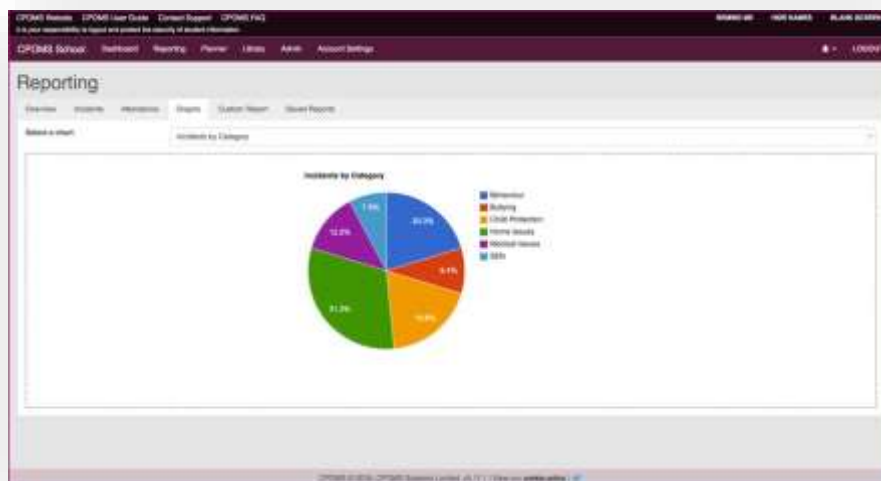
It's important therefore to consider exactly what your web filter is logging.

-  Are all requests authenticated?
-  Are all requests logged, including video and image assets – or just the domain?
-  Are these logs stored in an appropriate location?
-  Are these logs stored in an industry standard format like JSON?
-  Are logs kept intact, or is anything discarded to save space?

It's not essential for legislation to answer yes to all questions, but we feel it is essential for the safety of our children. Filter logging is important for satisfying law enforcement enquiries, but it's also important for safeguarding incidents, trends and sharing information with DSL colleagues. A high-quality education-focussed filter such as Smoothwall will offer the level of logging we at Garswood need. Many other

standard filters will offer basic reports and little else.

Garswood uses both Smoothwall reporting and CPOMs to record actions that have occurred in school under '**Internet Safety Concerns**' these can be compared and connected to other incidents if there is a correlation.



E-safety solutions for schools:

Garswood have opted for Smoothwall Optimum - a strong digital safety culture with Smoothwall's suite of e-safety solutions for schools, designed to keep students safe.

Digital safety in schools:

Simply meeting the minimum statutory requirements for e-safety doesn't protect us as a school or our children's needs, from digital risk in today's climate. It requires a multi-level approach.

In the case of St Helens and Garswood an effective e-safety infrastructure is made up of six harmonising components that combine to support students, staff and network safety - at every touchpoint. These include **comprehensive web filtering, firewall protection, digital monitoring**, digital record keeping, classroom management and e-safety training for your whole school community.

E-safety solutions for schools: A complete suite

We believe it is important that whether you're an IT, safeguarding leader or a teacher, Optimum gives Garswood end-to-end digital safety. This solution helps prevent harmful content before it's seen, predict incidents before they become real, and ensure students leverage the full benefit of internet learning without losing focus. Deploying all six solutions provides clear evidence of a robust, highest quality, digital safeguarding provision.

"I can't praise Smoothwall Monitor - Managed Service enough! It's not only made my life a lot easier, but it really does have the ability to transform lives because it gives me time to act."

DSL

King Harold Academy

Address	Business details	Contact
Smoothwall Second Floor, 2 Whitehall Quay, Leeds, LS1 4HR	VAT Registration Number: GB 282 7111 11 Smoothwall Limited is registered in the United Kingdom under... Company Number : 4298247	UK: 0800 047 8191 Overseas: +44(0) 113 539 7506 Email: enquiries@smoothwall.com

Garswood Filtering and Monitoring Checklist:

In line with the **KCSIE 2023** - [DfE filtering and monitoring standards in schools and colleges](#), this checklist has been developed to ensure Garswood meets the required standards. Working alongside our Filtering and Monitoring Policy, this checklist provides a summary record of checks highlighted within the standards.

Last updated:	Date:	September 2023	Name/Position:	Les Moon Computing Lead
---------------	-------	-----------------------	----------------	----------------------------

Roles and Responsibilities:

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Ian Green - Computing governor Jill Braithwaite - SEN governor
Senior Leadership Team Member	<p>Responsible for ensuring standards are met:</p> <ul style="list-style-type: none"> • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of provision • overseeing reports <p>Ensure that all staff:</p> <ul style="list-style-type: none"> • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns 	Pam Potter - Head teacher & DSL Les Moon - Computing lead & SLT Andrew Yearsley - Deputy head Lucy Myatt - SENCO & SLT Sue Bagshaw - SLT
Designated Safeguarding Lead	<p>Lead responsibility for safeguarding and online safety, overseeing and acting on:</p> <ul style="list-style-type: none"> • filtering and monitoring reports • safeguarding concerns • checks to filtering & monitoring systems 	Pam Potter - Head teacher & DSL
IT Service Provider	<p>Technical responsibility for:</p> <ul style="list-style-type: none"> • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems 	Maxine Morris - Schools ICT Manager Chris Smith - Schools ICT Infrastructure Manager Lee Pearson - Schools ICT Primary Team Manager

Reviewing your filtering and monitoring provision:

Filtering System	
Filtering Provider and System	SmoothWall Filtering
Date Procured	May 2012
Date last reviewed	January 2025

Monitoring System	
Monitoring Provider and System	SmoothWall Filtering (Reporting Service)
Date Procured	May 2012
Date last reviewed	January 2025

Review Team	Chris Smith - Schools ICT Infrastructure Manager Lee Pearson - Schools ICT Primary Team Manager	Pam Potter - Head teacher and DSL Les Moon - Computing lead
Review Date	September 2024	
Previous Review Date	N/A	
Link to last review	N/A	

Review Checklist	
the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)	
What your filtering currently blocks or allows & why	Y - staff are aware and report to DSL and record on CPOMS if needed
Any outside safeguarding influences, e.g. county lines	Y - staff have had training on safeguarding, county lines and online safety through the National College.
Any relevant safeguarding reports	Y - CPOMS and verbally report to DSL
The digital resilience of your pupils	Y - GIST Team and pupil voice
Teaching requirements, for example, your RHSE	Y - PSHE curriculum map and online safety map
The specific use of your chosen technologies, including Bring Your Own Device (BYOD)	Y - also present in the Garswood trainee handbook.
Related safeguarding or technology policies	Smoothwall Filter Monitoring & Filtering policy Online Safety Policy
What checks are currently taking place and how resulting actions are handled	Tested daily by ICT Support
All staff know how to report and record concerns	Y - CPOMS and verbally report to DSL
Filtering and monitoring systems work on new devices and services before release to staff / pupils	Y - all devices imaged and put on the network by the IT team before given to staff.
Blocklists are reviewed and they can be modified in line with changes to safeguarding risks	Y - By the IT Team, and emailed to DSL, deputy and Computing lead when there has been a breach. This is always followed up verbally and with a CPOMS entry.

Recommendations / Mitigating Actions

We recommend that schools use individual logins for pupils, especially at KS2, when using computers, rather than generic class/year logins so that the filtering system can identify individuals. We appreciate this may not be practical at FS and KS1 ages. If you are not using individual pupil logins speak to the ICT Support team who will facilitate this.

Use of iPads and other tablet devices will not identify an actual user of the device as there isn't a login to the device. The report will contain the IP Address of the device which IT can correspond to device. Schools need to have processes in place for recording which device was used by which user for these to be cross-referenced against reports. Schools ICT Support are investigating alternative approaches to this issue.

Data Protection Impact Assessment:

Schools that have a technical monitoring system will need to conduct their own Data Protection Impact Assessment (DPIA) and review the privacy notices of third-party providers

Link to DPIA	
Conducted by	Pam Potter - Head teacher and Designated Safeguarding Lead
Date conducted	September 2023

Regular Reports:

Type of Report	Filtering / Monitoring
Producer of report	Chris Smith - Schools ICT Infrastructure Manager
Recipient of report	Pam Potter - Headteacher and Designated Safeguarding Lead
Frequency of report	Weekly, immediate notifications of incidents regarding adult content and self-harm

Monitoring data is received in a format that your staff can understand	<input checked="" type="checkbox"/>
Users are identifiable to the school / college, so concerns can be traced back to an individual, including guest accounts	<input checked="" type="checkbox"/>

System Checks:

Filtering System				
Date checked		31/08/2024		
Checks conducted by		Lee Pearson - Schools ICT Primary Team Manager		
Device	Location	Logged in as	Check Conducted	Result
SCH-ICT-ED2702	St Helens Schools Data Centre	lee.pearson	888.com	Blocked

Confirm your filtering provider is:

• a member of Internet Watch Foundation (IWF)	Y
• signed up to Counter Terrorism Internet Referral Unit list (CTIRU)	Y
• blocking access to illegal content including Child Sexual Abuse Material (CSAM)	Y

Monitoring System

Date checked		31/08/2024		
Checks conducted by		Lee Pearson - Schools ICT Primary Team Manager		
Device	Location	Logged in as	Check Conducted	Result
SCH-ICT-ED2702	St Helens Schools Data Centre	lee.pearson	888.com	Blocked

Policy Reviewed - **January 2025**- Les Moon (IT lead) and Pam Potter (DSL)

Next Review - January 2026