St Bertelines C of E Primary School

Halton Borough Council

ONLINE SAFETY & SAFEGUARDING – WEB FILTERING GUIDE

HBC ICT Services – Learning Environment

Name of policy	Web Filtering Guide – Learning Environment
Author	Service Lead – Learning Environment
For approval by	Divisional and Service Managers, Software and Hardware Division, ICT Services
Date of approval	N/A
Frequency of review	Annually (or as DfE policy dictates)
Next review date	August 2024
Total No. of pages	12
Comments	Version 1

Contents

USEFUL INFORMATION

APPENDIX 1 – Forms Smoothwall

Authorisation Form SCOPE

OF THE GUIDE

This Web Filtering Guide outlines Halton Borough Council's responsibility and commitments to providing a web filtering solution that meets and exceeds the DfE Filtering and Monitoring Standard requirements.

The following applies:

- This guide only applies to learning providers who have signed up the current years Curriculum Support or Web Filtering SLA.
- If the learning provider uses an external ICT Support provider, they must follow the guidance from HBC ICT to install the web filtering certificate as recommended.
- The provider understands this guide only applies to devices connected to the schools network and does not apply to those connecting to private mobile networks. This should be reflected in the providers Mobile and Smart Technology and/or Child Protection Policies.
- The provider has a robust Online Safety and Child Protection Policy.

This document is designed to help schools and stakeholders understand the web filtering solution and SLA provided by HBC so they are confident their establishment complies with DfE statutory regulations and guidance.

DFE REQUIREMENTS

The DFE Filtering and Monitoring Standards outline the requirements for educational leaders to ensure their establishment has an appropriate filtering and monitoring system in place. To meet the requirements your establishment must:

- Identify and assign roles and responsibilities to manage your filtering and monitoring systems
  - Review your filtering and monitoring provision at least annually.
- Your filtering should block harmful and inappropriate contact without unreasonably impacting teaching and learning.
- You should have effective monitoring strategies that meet the safeguarding needs of your school or college.

HBC has taken the necessary steps to procure, provide and support a web filtering solution appropriate for education providers. This guide provides guidance on how to meet the requirements listed.

HBC WEB FILTERING SLA STATEMENT

The filtering service we provide to school must meet all DfE requirements and guidelines. Our Web filtering is provided by a 3rd party provider Smoothwall. Smoothwall have submitted responses to the UK Safer Internet Centre (as recommended by the DfE) which details how its product meets the national defined "appropriate filtering" standard. These responses can be found here:

smoothwalls-appropriate-filtering-for-education-settings-filtering-provider-response-july2022.pdf (d1xsi6mgo67kia.cloudfront.net)

From the responses provided we are confident this solution meets and exceeds the recommended guidelines and requirements expected by the DfE.

2. ROLES AND RESPONSIBILITIES

Your establishment must meet the following standard: "you should identify and assign roles and responsibilities to manage your filtering and monitoring service". The DfE recommend the following roles and responsibilities:

Head Teachers and Senior Leaders Responsibilities

Head teacher and senior leaders are responsible for:

- Procuring filtering and monitoring systems
- Document Decisions on what is blocked or allowed and why
- Reviewing the effectiveness of your provision
- Overseeing reports
- Ensuring all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns.

Designated Safeguarding Lead

The Designated Safeguarding Lead is responsible for:

- Reviewing filtering and monitoring reports.
- Taking action where appropriate.
- Dealing with Safeguarding concerns.
- Document any requested changes to the filtering system, including reason for request Working with HBC to carry out reviews and checks.

Halton Borough Council ICT Network Managers

HBC ICT Managers have technical responsibility for the following:

- Procuring filtering and monitoring systems from a solution provider.
- Raise any concerns regarding the technical infrastructure to the Head Teacher immediately.

- Ensuring the web filter and monitoring system is maintained and managed at all time.
- Ensuring the web filter and monitoring reports are setup and provided to the relevant people.
- Carry out regular reviews and checks to ensure the web filter and monitor is working effectively.
- That any concerns or checks are actioned as soon as possible.
- Document any changes to the filtering system.

HBC ICT Managers are also responsible for providing all services as listed in the Web Filtering SLA (see point 4 for further information)

3. HBC WEB FILTERING SOLUTION

Your DSL must meet the requirement "understanding the filtering and monitoring system and processes in place". Below is a description of the web filtering solution and Service currently in place.

3.1 What devices are filtered?

All school owned devices are automatically enrolled to the web filter. Any device on your network, school owned and private, that does not have the Smoothwall certificate installed is automatically blocked from accessing the internet on your network. This is applied at all times

3.2 How does the filter work?

Smoothwall is a real time web filter and monitor system. It scans the content and context of every web page or internet search for unwanted material. Where unwanted material is found it blocks access to the web page and triggers an alert.

There are a number of categories that are blocked to comply with Prevent Agenda and MCSIE requirements. As a minimum the categories blocked are:

- Bullying
- Discrimination
- Drugs / Substance abuse
- Extremism
- Illegal
- Malware / Hacking
- Pornography
- Piracy and Copyright theft
- Self Harm / Suicide Violence

There are other categories which are also blocked to comply with other DfE online safety requirements, e.g. Social Media. The appropriateness of these sites are a matter for individual providers and we will unblock/block these upon request.

The level of restriction currently in place is based on the group the user is assigned to. It is the customers responsibility to ensure the members of these groups are up-to-date. Where we have not been provided with this information the user will be assigned to the least privilege group, e.g. they will be filtered as a student.

3.3 How does the monitor work?

Monitoring reports can be generated in real time and on request by the providers SLT or DSL. Monitoring reports can be sent to any user the school specify, but should follow DfE guidelines on roles and responsibilities (see above).

There are two types of real time monitoring reports – immediate and general alerts.

- Immediate alerts are generated when a user attempts to access or searches for a webpage whose category is listed in 3.1. Authorised persons will receive an immediate email to alert them.
- A general alert is triggered when a blocked category other than those listed in 3.1. is triggered. The authorised person(s) will receive an email to alert them the following day. This ensures the authorised user can prioritise reports accordingly.

The monitoring system can also provide the last 30 days internet history for any person using our web filtering system, adult or student.

3.4 What happens when a page is blocked?

When a user attempts to access or search for restricted content, Smoothwall will present the user with a 'block page'. The block page will advise the user "the content of the page does not comply with acceptable usage policy", it will then display the following information:

- the category the page has been classified as
- the group the user is part of
- the IP/URL of the web page
- reason the website was blocked.

The above information is also sent to Authorised person(s), along with user identifiable information. The monitoring data is received in a clear format so that concerns can be traced to back to an individual.

3.5 Who can receive reports and who can request changes?

- Upon taking this SLA the learning provider must complete an Authorised Persons form. This form provides us with the name(s) of the users who should receive Smoothwall Alerts for the school (See appendix 1). We advise a minimum or 2 members of staff receive these reports. It is the school's responsibility to ensure this list remains accurate.

- The users listed on this form will also be authorised to request changes to the filtering settings. We will not make changes unless requested to by an authorised person.

3.6 Does the filter over block?

Smoothwall uses Dynamic Content Filtering, and examines the entire content of a web page, not just what is displayed on the screen. As such Smoothwall has a tendency to over-block, but we strongly believe it is better to block some safe sites than risk allowing dangerous content through.

However, so you comply with the new guidance we will be making changes to Smoothwall in the very near future so your DSL has the ability to change the blocked categories more easily. In the meantime if a website is incorrectly categorised, Smoothwall has an easy way for us to report this error and have it changed.

3.7 Can HBC decline a request to unblock a website?

If providing access to a website would compromise the security of the network we can decline a request, but we will provide written reasons for our decision. Where we believe allowing access to a website could potentially leave you "none compliant" we will discuss this with your establishment's leadership team.

3.8 How can I view what is blocked?

You can view which categories are currently blocked whilst logged in as a user by going to http://test.mysmoothwall.net

3.9 How often are the categories updated?

The system is setup to automatically download updates. It is checked on a weekly basis to ensure it has the latest updates. We also monitor national security alerts and implement further changes and updates as required.

The latest block-list and content modification list can be found here: Blocklist Categories and Content Modifications List – Knowledge Base (smoothwall.com).

4. Monitoring and Review

We monitor and review the filter at all times to ensure it is operating correctly. The DfE advise "you should review your filtering and monitoring provision at least annually" and "your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning". To ensure you remain compliant we review this provision throughout the year.

How often will we review the filter/monitor?

The DFE Standard requires for a filter/monitoring provision to be checked at least annually. Under HBC SLA we will review Smoothwall:

- Daily to ensure it operating correctly.
- On request by the SLT or DSL or ICT Technician.

- In response to an incident or concern.
- When a significant change takes place, including technology upgrade, policy or legislation change.
- Annually.

How will we test the filter/Monitor?

- Upon request, we will test the filter using the lastest recommended DFE guidelines, including filtering test: Test Your Internet Filter | SWGfL Test Filtering
- We will check against the latest security and social media threats.

On a daily/weekly basis we will also ensure that:

- Smoothwall is operating correctly. Smoothwall filters are up-to-date.

4.1 Incident Reporting

Incidents can be reported by any member of school staff and will be treated with the highest priority. Incidents can be reported via email, phone or in person to the Service Lead of HBC Learning Environment, IT Helpdesk or reported to any school technical or SIMS Officer.

An incident can be any of the following:

- Unsuitable material accessed or suspected to have been accessed
- They require access to material which may generate alerts
- There is a failure in the software or abuse of the system They are being restricted unreasonably

All incidents will be reviewed with the schools DSL.

4.2 Incident Reviews

Incidents will be reviewed with the DSL to ensure you meet the standard “Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning”.

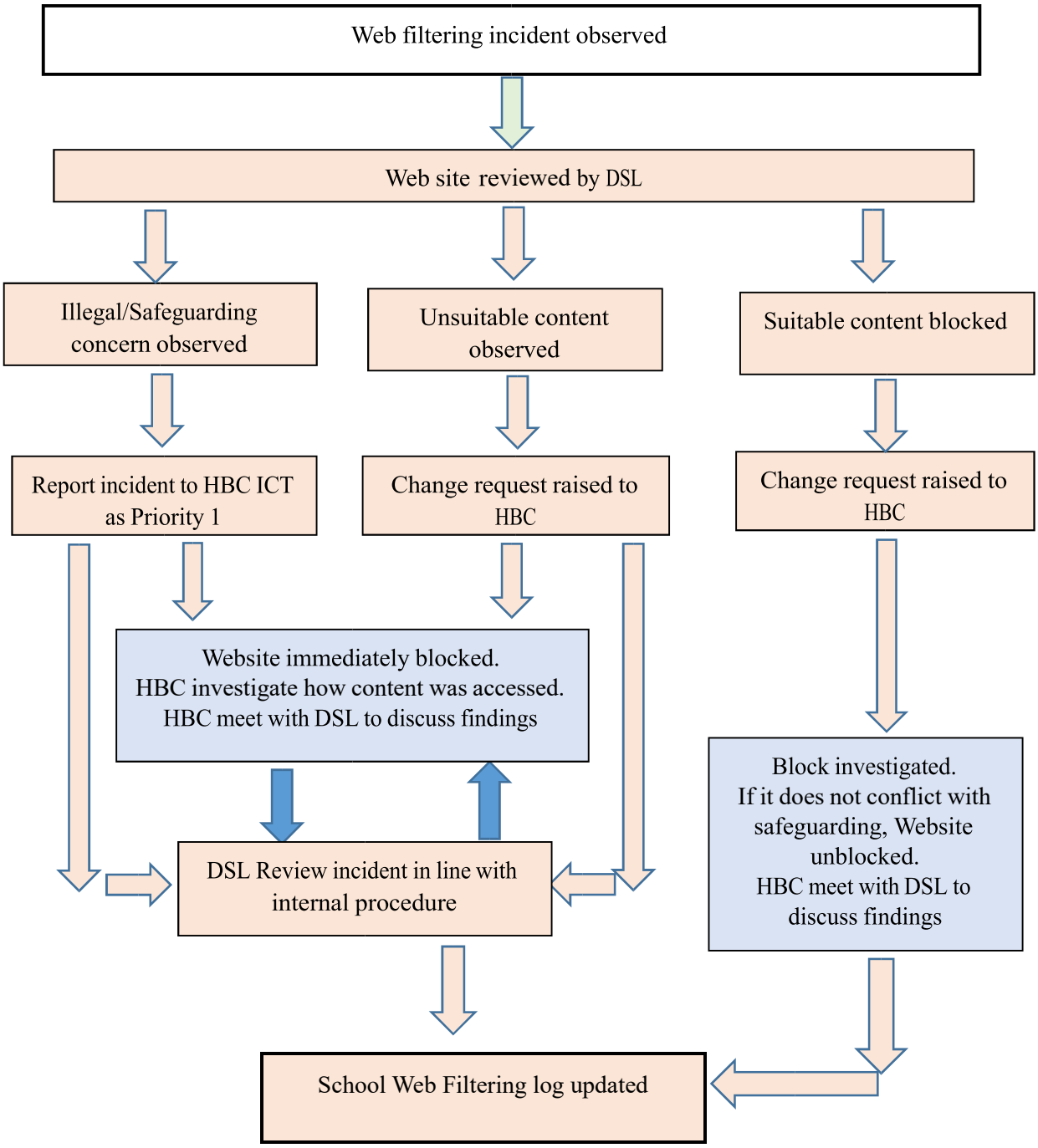
4.3 Change request / change log

Any request for change must be submitted by authorised persons. Requests for changes must be submitted in writing together with a reason for the change. It is advised by the DfE for schools to maintain a “change log”.

However, If we believe providing access would beach Safeguarding legislation, or would put the network/device at risk of virus, we reserve the right to refuse the request and seek advice from HBC Safeguarding Team and/or HBC Security Team.

4.4 Incident Review Process

The chart below is a suggested model for reporting incidents, but can be adapted for your establishments needs:



Incident reviewed again at next review

5. Effective Monitoring Strategies

Your establishment should have effective monitoring strategies in place that meet the safeguarding needs of your establishment. Our Web Filtering Service can be adapted to meet the requirements you identify. See below links recommended by the DfE to meet this requirement for your environment.

USEFUL INFORMATION

Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

2023 Appropriate filtering and monitoring definitions published - UK Safer Internet Centre

Appropriate Filtering - UK Safer Internet Centre

Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf (ncsc.gov.uk)

Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) Online Safety Self-Review Tool for Schools | 360safe

Cyber security training for school staff - NCSC.GOV.UK

School cyber security questions for governors - NCSC.GOV.UK

Smoothwall Report Authorisation Form – to be completed by Head Teacher/DSL only

Name of School: St Berteline's C of E Primary School

Head Teacher name: Mrs Sheridan Moss

Signed: Date May 2024

The following users have been authorized by the Head Teacher to receive Smoothwall Reports for the above named school:

Nominated Staff Member 1:

Name: Mrs Sheridan Moss

Position: Headteacher

Contact Email: sec.stbertelines@haltonlearning.net

Authorised to request changes: Yes

Nominated Staff Member 2:

Name: Admin Office

Position: Business Manager/Admin Officer

Authorised to request changes: Yes

Nominated Staff Member 3:

Name: Wearesync

Position: Support Desk

Contact Email: support@wearesync.co.uk

Authorised to request changes: No

Terms and Conditions:

- The reporting of user activity is limited to devices accessing the Internet on Halton Borough Councils Schools network.
- The monitoring of user activity and Smoothwall® reports is the responsibility of the school.
- Where a user has accidently or deliberately tried to access restricted content, it is the responsibility of the school to take appropriate action.

- Where we feel that allowing access through the firewall or filter would constitute a serious risk to the school network, security, GDPR or safeguarding, we reserve the right to seek advice from HBC e-Safety Lead Officer and deny your request, or block access to our service.