FILTERING AND MONITORING ONLINE SAFETY POLICY

This Policy was approved by Governors in:	February 2024
This Policy was shared with staff in:	February 2024
Implementation of this Policy will be monitored by:	The Headteacher
Policy Review Date:	February 2024
Date for next Review:	**February 2025**

This policy is part of the School's Statutory Safeguarding Policy
Any issues and concerns with online safety must follow the school's safeguarding and child protection processes

We follow the LGFL School Online Safety Policy and have adapted it to fit the needs of our school

This document includes links to relevant websites
An electronic version will be issued to those wishing to utilise these links

1. INTRODUCTION AND OVERVIEW

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Poverest Primary School's filtering service is provided by LGFL and administered by Blue Fox Systems with the knowledge of the headteacher.

Blue Fox is an official technical partner of LGFL and supports several schools.

Our Computing Lead looks after the web filtering for school and will ensure that:

- The service is maintained and accessible for all school sites to use.
- All relevant safeguards are being met.
- School is taking necessary precautions to ensure the service provided is appropriate.

Also, provide investigation of any web filtering related issues including:

- Access to websites containing inappropriate or potentially harmful material.
- Access to websites containing educational or related material deemed appropriate for school.
- Provide web access reports on an annual basis. Work with Blue Fox to work together to ensure that the UK Safer Internet Centre checklist is followed.
- LGfL web filtering service meets and exceeds the Ofsted guidelines. The solution is constantly updated via national feeds from the wider internet community to ensure that as new websites are created they are categorised and sanctioned accordingly.

Above the web filtering aspect of the service, work with Blue Fox to also provide the following features:

- Application Control – this stops some applications running which utilise peer-to-peer (file-sharing) features.
- Intrusion Prevention – this is aimed at stopping hackers from gaining access to your endpoints.
- Website Certificate Inspection – this checks websites to ensure any certificates are valid and up to date. This stops users from accessing malicious websites or websites that are not properly maintained.

Schools (and registered childcare providers) in England and Wales are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering” (Revised Prevent Duty Guidance: for England and Wales).

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

Department for Education’s statutory guidance ‘Keeping Children Safe in Education’ obliges schools and colleges in England to “ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system” however, schools will need to “be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

From the information provided to us by our supplier Blue Fox, we are confident that the web filtering solution as configured meets the current DfE guidance.

2. AIMS AND OBJECTIVES

Each school will have its own unique demands and use of the internet. However, all schools must ensure they appropriately safeguard staff and pupils through an effective online filtering and monitoring regime.

3. REQUIREMENTS OF ONLINE FILTERING AND MONITORING

All schools must ensure that internet systems are robust and appropriate for use. Schools are required to follow the guidance below:
Poverest Primary School needs to be able to demonstrate how its systems manage effective filtering and monitoring by the completion of an annual safety check, including filtering and monitoring.

Poverest will provide checklists/documentation for use in schools.

- LGfL - appropriate filtering for educational settings (Appendix 1).

The review checklist is completed at the beginning of every school year. Weekly checks using Webscreen occur every Friday and are untaken by the headteacher. Support is given by Blue Fox if required.

The completion of these checks will allow all leaders to construct a risk assessment that considers the risks that both children and staff may encounter online.

4. ROLES AND RESPONSIBILITIES

The responsibility for the management of the school's filtering and monitoring policy will be held by the E-Safety Coordinator supported by the Computing Lead. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- Be logged in change control logs.
- Be reported to a second responsible person (Headteacher).

All users have a responsibility to report immediately to the E-Safety Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, that they believe should have been filtered. Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

5. EDUCATION/TRAINING/AWARENESS

Pupils will be made aware of the importance of filtering systems through the E-Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- Signing the AUP.
- Induction training through National Online Safety.
- Staff meetings and briefings.
- Information posted in the Staff Room.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement.

6. CHANGES TO THE FILTERING SYSTEM

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the DSL who will decide whether to make school-level changes (as above). If it is felt that the site should be filtered (or unfiltered), the E-Safety Co-ordinator should contact the Computing Lead with the URL.

7. MEETING DIGITAL AND TECHNOLOGY STANDARDS IN SCHOOLS

7.1 Roles and responsibilities to manage your filtering and monitoring systems.

- DSL: Paul Haylock and Kerry Boorman
- IT Provider: Blue Fox Systems
- Filtering and monitoring system: LGfL

7.2 Review of filtering and monitoring by DSL and IT provider twice yearly. In the Autumn when the Annual Safety Check occurs and again in the Spring Term when the actions from the Annual Safety Check are reviewed.

7.3 The filtering system blocks harmful and inappropriate content, without unreasonably impacting teaching and learning.

- LGfL - Appropriate Filtering for Educational Settings (Appendix 1)

8. LINKS WITH OTHER POLICIES

This policy will be monitored as part of the school's annual internal review and reviewed on a three-year cycle or as required by legislature changes.

This policy links to the following policies and procedures:

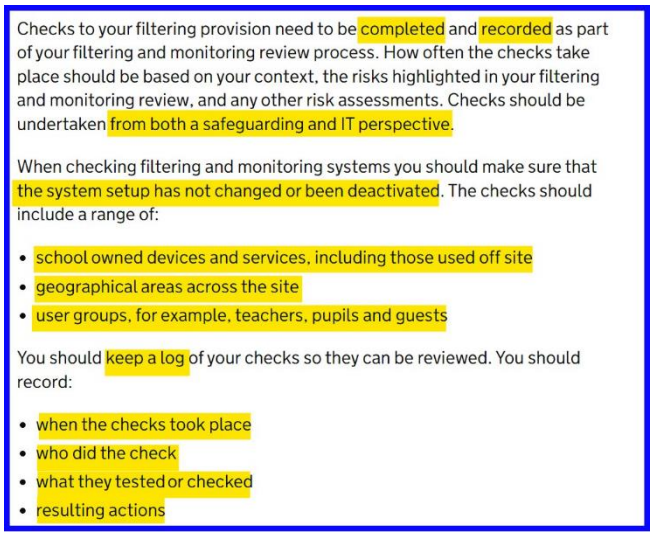
- Safeguarding Policy
- E-Safety Policy

APPENDIX 1

Web Filtering Checks Template

The DfE Filtering and Monitoring Standards (referenced in KCSIE 2023) require schools to perform ***regular checks*** on filtering systems so that "governing bodies and proprietors have assurance that systems are working effectively and meeting safeguarding obligations".

Check versus review – are they the same?
These are not the same things – checks are regular and operational: ensuring devices, platforms and accounts continue to be filtered as planned; the review is annual (or whenever major changes are made) and strategic: you may wish to combine this with your annual online safety audit. See safefiltering.lgfl.net for more information on the differences.



Checks to your filtering provision need to be completed and recorded as part of your filtering and monitoring review process. How often the checks take place should be based on your context, the risks highlighted in your filtering and monitoring review, and any other risk assessments. Checks should be undertaken from both a safeguarding and IT perspective.

When checking filtering and monitoring systems you should make sure that the system setup has not changed or been deactivated. The checks should include a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

You should keep a log of your checks so they can be reviewed. You should record:

- when the checks took place
- who did the check
- what they tested or checked
- resulting actions

How often?
There is no definition on how regular checks might take place but LGfL recommends either monthly or half-termly as a useful interval.

What are we checking?
The next page has a pro forma to edit and use for checks, but first consider and document who will complete them and how, how many devices/accounts to check and how to log and follow up on necessary actions. It is for schools to make these decisions based on your context and need.

Who needs to do it?
The DSL has overall responsibility, but that does not mean they need to carry out the checks. Safeguarding teams should work with other senior leaders and technical teams to work out which checks are most helpful in your setting and the answers to the questions above, but the actual checking can be delegated, so long as results and actions are reported back to the safeguarding team for discussion and review of next steps. Remember also the key role of ALL staff in feeding back on any issues that they spot with accessing or not being able to access content.

What are we trying to find out?
In essence, you want to know:

- Are key things blocked?
- Are we 'overblocking'?
- Is filtering ACTIVE EVERYWHERE (all connections & all devices & all users)?
- Is Safe Search ENFORCED (i.e. can't be turned off) EVERYWHERE (as above)?
- Are there concerns about students bypassing blocks?

Before you start, make sure you have liaised with your tech team to identify all types of user, device, account and physical location (remember portacabins, trolleys, home devices, guest networks and BYOD and the most recent new or rebuilt device) and have scheduled your checks to cover all of these over the academic year.

Use the following proforma to log the checks that take place in your school. Feel free to edit this template and add your school logo but please do not remove the LGfL branding or copyright notice.

Time and date:		**Completed by:**	
Device type and location checked: *(note device IDs)*		**Type of user account / system checked:**	

		Any issues? ✓ or ✗	**Actions** *(Who, what, how, by when)*
1	**Have all actions from the last filtering checks been completed?**		
2	**Is filtering active?** *Non-LGfL school* – ask your technician/provider how best to do this. *LGfL school* – attempt to visit testhomeprotect.lgfl.net / http://wsblock.co.uk * (they should show a block page, NOT load, showing you filtering is active). While on the block page, click to see more information and double check you are on the correct policy, e.g. student policy for a student login (if your provider does not have this on the block page, ask how you can test this).		
	Is the correct policy assigned? *Non-LGfL school* – ask your technician/provider how best to do this. *LGfL school* – while on the block page (eg via above), click to see more information and double check you are on the correct policy, e.g. student policy for a student login (if your provider does not have this on the block page, ask how you can test this).		

3	**Are the expected categories blocked?** *Non-LGfL school* – ask your technician/provider how best to do this. Beware, if you visit inappropriate sites for testing you should get approval first, log this action for your own protection and consider carefully which to use (e.g. guinness.com, paddypower.com); do not visit real adult sites for testing. *LGfL school* – we have test pages for multiple categories (eg adult/gaming) that you can safely attempt to visit. See note above regarding visits to real sites. Test pages are available via testhomeprotect.lgfl.net or http://testwebscreen.co.uk *		
4	**Are the relevant illegal sites blocked?** Use the Safer Internet Centre's tool at testfiltering.com (select the school button then 'run filtering test'). This covers the IWF and Home Office terrorist and sexual abuse lists. Your provider will also have filed a submission to the Safer Internet Centre with the lists it blocks. *LGfL schools* – note also that LGfL also blocks the City of London Police PIPCU list for pirated film material		
5	**Is your YouTube mode as expected?** Which of the two restricted modes can you see – visit youtubemode.lgfl.net to test this. Find out more about YouTube modes at youtube.lgfl.net		

6	**Is Safe Search on and ENFORCED for all search engines you use?** It is vital that this cannot be turned off by users. For Google, visit safesearchcheck.lgfl.net and be sure you cannot toggle it off. (You may wish to block the 'search engine' category for all users and override this only for the one or several which you permit and can guarantee an enforceable safe search for)		
7	**Is a website or page which you specifically blocked / unblocked recently or after the last set of checks correct for all users/accounts/devices?** Remember this may be different for different Key Stages or classroom v office staff for example.		
8	**Have you asked staff & pupils if they have recently been unable to access educational sites or stumbled across inappropriate sites?** An email reminder to staff whenever you do these checks is wise. Consider what system there is to report instantly (an online form may be better for their responses than email)?		

** Please note that sites marked http for checking categories etc must be http not https – this is deliberate and is to do with showing individual pages for schools whether they have decryption activated or not. You may be given a browser warning before visiting these pages (which you should otherwise not ignore).*