Appendix 1 - Filtering and **Monitoring** Policy and Procedures

1.1 Introduction

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 regularly review their effectiveness" 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"* 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*."

Ofsted concluded as far back as 2010 that "Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves."

To further support schools and colleges in England, the Department for Education published Digital and Technology standards.

1.2 Roles and Responsibilities

The school works in partnership with the IT service provider *EXA Networks Quantum* to ensure that the school infrastructure/network is as safe and secure as is reasonably possible. DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage filtering and monitoring systems.

Role	**Responsibility**	**Name / Position**
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Philip Ashdown
Senior Leadership	Team Member Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	Caron Short working with headteacher Lisa Mayes and Trust IT manager Chris Webb
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which includes overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems	Caron Short

IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	EXA Networks Surf Protect Quantum
All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report 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 the 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	

1.3 Policy statement

- There is a filtering and monitoring system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content.
- There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.
- Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.
- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change.
- Mobile devices that access the school's internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.
- *The school has provided enhanced/differentiated user-level filtering through the use of* EXA Networks Quantum *filtering system. User based filtering is used, so Teaching Staff have different access rights to Pupils*

1.4 Filtering Procedures

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, as online content changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use.

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and other illegal content lists. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

The filtering system used in our school is up to date and applied to all:

- users, including guest accounts

- school owned devices
- devices using the school broadband connection

This system:

- filters all internet feeds, including any backup connections
- is age and ability appropriate for the users and is suitable for educational settings
- handles multilingual web content, images, common misspellings and abbreviations
- identifies technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them
- provides alerts when any web content has been blocked
- is regularly updated

1.5 Monitoring Procedures

Monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows review of user activity on school devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing prompt action to be taken.

Our monitoring strategy includes:

- physical monitoring by staff watching screens of users
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon.

1.6 Filtering and Monitoring Review and Checks

Strategic review

The filtering and monitoring provision is reviewed at least annually, as part of a wider online safety annual review, using the 360 degree safe tool, or when:

- a safeguarding risk is identified
- there is a change in working practice, e.g. remote access or BYOD (BYOD is not permitted at Lethbridge)
- new technology is introduced

The review is conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider.

Operational review

In addition to the annual review of filtering and monitoring, checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments.

Checks will be undertaken from both a safeguarding and IT perspective.

In our school, we complete the following checks:

1. a review of the monitoring logs to check for patterns and themes which may arise from user access and cause concern. These are completed termly

2. Checks of the filtering systems are performed on 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

Checks are completed on class log ins on laptops and computers that are used by children. Browser history is removed so pupils can see the test searches.

Logs of checks are kept so they can be reviewed. These record:

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

A check using the SWGfL Test Filtering website is also completed three times a year.

1.7 Changes to Filtering and Monitoring Systems

Users may request changes to the filtering and monitoring systems through the headteacher who will liaise with the Blue Kite Trust IT manager to determine the suitability and safety of any change. Any changes will not affect statutory DfE guidelines.

1.8 Training/Awareness

It is a statutory requirement in England that staff receive training, at least annually, about safeguarding, child protection, online safety and filtering and monitoring.

Governors, Senior Leaders and staff are made aware of the expectations of them:

- at induction
- at whole-staff/governor training
- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

Learners are made aware of the expectations of them:

- in lessons, principally **through the computing and PHSE curriculum, but in all areas where any IT is utilised; in termly assemblies**
- through the acceptable use agreements

Parents are informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions and communications such as through the school newsletter etc.

This appendix is informed by the Department for Education (DfE) guidance, Keeping Children Safe in Education, and the Digital and Technology Standards and is based on a template from the South West Grid For Learning (SWGfL).

Date: 01.07.2024