

Keeping Children Safe In Education Sept 2023

Following the update to KCSIE in 2023 there have been significant changes to how schools deal with online safety and how they manage their filtering and monitoring. Historically, the IT Support Team have administered the filtering for schools. To comply with the new guidance, schools need to take a more active role in managing their filtering and monitoring. The updates and implications for you as a school are detailed below:

1. Role & Responsibilities

- 1.1. The first significant change is that schools now need to identify who has overall strategic responsibility for filtering and monitoring. This should include a member of SLT and a governor.
- 1.2. KCSIE also identifies that the **DSL** should take lead responsibility for safeguarding and child protection (including online safety and understanding the **filtering and monitoring** systems and processes in place).
- 1.3. The DfE have clearly identified the responsibilities for both the school and us as the IT Support Provider. These are detailed below:

School's Responsibilities	IT Support Provider's Responsibilities
Procuring filtering and monitoring systems	Maintaining filtering and monitoring systems
Documenting decisions on what is blocked or allowed and why	Providing filtering and monitoring reports
Reviewing the effectiveness of your provision	Completing actions following concerns or checks to systems
Overseeing reports	
Making sure that all staff Understand their role Are appropriately trained Follow policies, processes and procedures Act on reports and concerns	Work with the senior leadership team and DSL to: Procure systems Identify risk Carry out reviews Carry out checks

2. Reviewing your provision

- 2.1. KCSIE identifies a need for *'appropriate filters and monitoring systems'* to support schools in determining whether their filtering and monitoring solution is appropriate. The UK Safer Internet Centre have produced guidance for schools to refer to when considering whether their solution is appropriate. They also invite suppliers to demonstrate how their solution adheres to their guidance and Smoothwall's response is available [here](#).

- 2.2. The filtering and monitoring standards recommend reviewing your filtering provision on an annual basis and KCSIE identifies schools '*should consider carrying out an annual review of their approach to online safety*'. The two recommended frameworks for the audit are available via the links below:

[LGFL - School Online Safety Audit and Risk Assessment](#)

[SWGfL - 360 Online Safety Self-Review Tool for Schools](#)

If as a school, you choose to do a full online safety audit you would include the review of your filtering solution as part of this. Alternatively, if you choose not to complete an annual online audit, you must still review your filtering and monitoring provision.

- 2.3. As a Support Provider, we will support schools in their audits as required. To support schools in reviewing their filtering solution, we will send out a breakdown of how the filtering solution is categorised and which categories are allowed or blocked for teachers and pupils in your school.
- 2.4. The guidance states that SLT may decide to enforce Google SafeSearch to provide an additional level of protection for your users on top of filtering – this is forced on for all schools that we support by default. As part of the annual review of filtering we will include information about SafeSearch and confirm that you want it enforced (which we would highly recommend).
- 2.5. The guidance also recommends that schools make use of the filtering checker from SWGfL, this checks that Child Sexual Abuse, Offensive Language, Terrorism & Adult Content is blocked on the network. We would recommend all DSL's running the test and keeping a record of the test and results (via a screenshot with date/ time).

[Test Your Internet Filter | SWGfL Test Filtering](#)

- 2.6. Schools also need to make sure that staff are aware of how to report any concerns they have, should that be the filtering is allowing unsuitable content through or the filtering solution is too restrictive. Indeed, KCSIE identifies 'Over-Blocking' as a risk to a schools filtering solution. As a school, to ensure you are not over-blocking, agree your filtering categorisation and then monitor the number of unblock requests you receive from your staff. If you are seeing lots of requests, you may need to review your base filter.
- 2.7. The guidance also discusses reviewing the effectiveness of the solution. To do this, we would recommend undertaking monthly checks on sites you would expect to be blocked. To do this, a school should refer to their blocked categories and then search for sites that would fall under this category. For example, if you block social media, check Instagram is blocked (<http://instagram.com>).

3. Monitoring

- 3.1. As part of reviewing your provision, schools should again refer to the UK Safer Internet Centre's guidance, the link to Smoothwall's response to this guidance is available [here](#). Smoothwall's response highlights a potential risk for Bring Your Own Device (BYOD), however no school who we provide support to allow BYOD, so this mitigates the risk.
- 3.2. We need to send regular monitoring reports and alerts to each individual school's Digital Safeguarding Lead. To do this, we need you to confirm their email address. Alerts will be setup to send an immediate notification if there is a safeguarding risk (a child tries to access self-harm content for instance). In addition, monthly generic reports will be sent to the DSL detailing reports of access to all blocked sites.

4. References

Keeping Children Safe In Education, DfE – [Available here](#)

Meeting Digital and Technology Standard in School and Colleges, DfE - [Available here](#)

Appropriate Filtering for Education Settings, UK Safer Internet Centre - [Available here](#)

Appropriate Monitoring in Education Settings, UK Safer Internet Centre - [Available here](#)