FAQ about monitoring the Internet in schools

Recent guidance in the Keeping Children Safe in Education[1] paper from the DfE gives advice about monitoring the School internet connection[2].

This paper endeavours to define a difference between filtering and monitoring and explain the school's responsibilities.

What is the difference between filtering and monitoring?

Filtering is a technical solution to masking many of the sites that are available on the internet. This can either be completed for all the computers or for differentiated policy groups and therefore users in the school. Some users, such as technicians, need unfiltered access.

Even the best filter is not perfect and there have been many instances where unfortunate content and images have appeared on computers. Older learners and staff also do not like being restricted and can surreptitiously find ways of avoiding the filter.

Monitoring is looking at the reality of the situation to see which websites children and staff are attempting to access, checking that the filter is working and providing strategies that further ensure the safety of users. Your school Online Safety policy should mention that you monitor the use of the internet.

Why does my school need to monitor its internet connection?

The provision of an internet connection into a school automatically creates risks. It is within a school's responsibility to assess these risks. Despite most educational filtering systems being very good, there are places where issues can happen. Here monitoring can be used to safeguard and then to improve practices.

What is monitoring?

Monitoring is a mixture of strategies aimed at safeguarding users. It is a combination of physical and technological solutions suited to the circumstances of the school. It normally involves checking the search terms and sites used when users are on the internet and by its very nature is linked to filtering. In some schools monitoring could be implemented by only allowing supervised access.

In others where there is unsupervised access or risks have been judged to be greater it might involve technological solutions. Monitoring is reactive, but this does not diminish its importance.

---

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
[2] http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-and-monitoring/appropriate-monitoring

FAQ about monitoring the Internet in schools

What monitoring do I need if the users are supervised at all times?

In many small schools there is a common assertion that the users are supervised at all times. Adult supervision is a perfectly acceptable monitoring method but you must make sure that it is in place if for instance learners are allowed to use tablets during wet play or working alone in corridors.

Is there a difference between PCs and wireless devices such as tablets?

It is not necessarily the difference between the type of device, but the way in which they connect to the internet. The clue here is: Do you have to log in using a user name and password? If the answer is yes, then the system will produce a logfile against that user and this can be monitored. If the answer is no (as is the case with tablets) then it is far more difficult to trace the logfile against the user.

What about monitoring staff?

Staff use of the internet should also be monitored. They deserve the same amount of safeguarding as the learners. This includes the technical staff who might have unfiltered access.

What about the learners?

Learners monitor their use of the internet all the time. They should be taught what to do if they find things that they are not sure about. Older users could use tactics to 'bypass the proxy' (avoid the filter) and you should monitor to check that this activity is not taking place.

What about the parents?

As a parent you would expect your child's use of the intent to be monitored. If a child goes home and says that they accessed a questionable site on the school's internet connection, the school should be prepared to say how it monitors use and how it follows up issues.

Do we need to buy expensive solutions to monitor the internet?

The answer depends on the circumstances of the school and the existing provision of the school.

A Primary school that does not allow unsupervised learner use of the internet will need no more than a competent educational filtering package provided. The supervision can be deemed as sufficient monitoring.

A Primary school that is larger, or one that does allow unsupervised access by older learners, should consider the use of personal username and passwords so that all

activity can easily be traced. If tablets do not have the ability to have personal logins, then their use should be logged by writing down the name of the user against that tablet.

A Secondary school where the risk has been assessed as being minimal should have user based filtering and therefore personal logfiles.

A Secondary school that has wireless connectivity for Bring Your Own Devices (BYOD) should consider how they monitor its use.

A Secondary school where there is medium to high risk should consider the use of active monitoring services. These examine the network traffic of the school and then send reports to a nominated person.

What about personal devices?

Allowing personal devices (sometimes called Bring Your Own Device or BYOD) onto the school internet connection does not negate the need to monitor. Any use of your connection has to be monitored.

Does monitoring create work?

The quick answer is yes. The responsibilities of the school towards safeguarding are very important and cannot be ignored. Normally in larger Secondary school the monitoring would be carried out by the IT technicians, in a small Primary school it could be the safeguarding lead.

There is always a balance in the amount of work created and the effect of the monitoring. Monitoring must be effective and not onerous while maintaining everyone's safety.

What should I do?

The first thing to do is a risk assessment of your schools use of the Internet (See Appendix).

From that, create a list of the strategies that you have in place and highlight the steps that you need to take to make improvement.

Consider:

- Supervised access
- User based filtering
- Wireless connectivity (BYOD)
- Active monitoring services

If you have any questions, then get in contact with eLIM who will support you to support your learners and staff to be safe

Appendix – A risk assessment of a schools use of the Internet

Is my school using a filtering package from a provider who has self-certified on the Appropriate Filtering checklist[3]?	Yes/No
Are learners always supervised when using the internet?	Yes/No
Do users know the procedure if they find something inappropriate on the Internet?	Yes/No
Do all devices (PCs/Laptops/tablets) access the internet with a personal login?	Yes/No
Do we ban personal devices from connecting to the school internet feed?	Yes/No
Are any users with unfiltered web access monitored?	Yes/No
Am I secure that potentially vulnerable users in my school for whom I have concerns with regards to extremism, hacking, pornography, self-harm or other such issues are always monitored in their use of the internet?	Yes/No
Can I explain to a parent who expresses a concern the way in which the monitoring strategy of the school is as good as it could be?	Yes/No

If any of the answers to any of the questions are **No** then you need to consider how you could improve the way in which you monitor the internet connection.

If you have any questions, then get in contact with eLIM who will support you to support your learners and staff to be safe

[3] http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-and-monitoring/appropriate-filtering