white paper:
e-safety management

a balance between blocking and managing internet content in schools

Alan Mackenzie - January 2014

impero

contents

the author

Impero commissioned Alan Mackenzie to write this report.

Alan is an independent consultant working in the education and private sectors, specialising in e-safety and also the innovative use of technology to support learning. Coming from a local authority background he has in-depth knowledge and experience of the use of ICT in both an educational and business sense.

Alan is a strong believer that e-safety is an enabler: appropriate policy and processes, empowering the right education and the use of effective tools can help schools to innovate and educate without the fear of e-safety risk.

In this paper, Alan gives his thoughts and experience of the role of internet filtering software in schools as a tool to mitigate risk. Is this technology used correctly and is it appropriate? Can a better balance be achieved and if so, how?

Alan Mackenzie

T +44 (0) 1522 253 088
E alan@esafety-adviser.com

www.esafety-adviser.com

executive summary

As the use of new technology such as tablet devices, and online services such as social networking or social sharing, is being adopted in many schools there is the potential for an increase in risk to both the school and the student. Commonly it is an internet content filter that is used as the first (and sometimes only) line of defence. But is this still appropriate technology in an age when schools are using more and more online services?

Some schools are real pathfinders; they are adopting new ways of learning, using ICT to enhance or extend that learning. This is great to see; the use of ICT should never be about learning to "use the tool", but using it "as a tool" to enhance something else. In the context of e-safety, one of the outcomes of using these tools is that students can be more empowered with a life-skill far more effectively than by watching a few videos; learning by doing, not learning by telling.

But whilst internet filtering software is used as a first line of defence, commonly it is also one of the more frustrating services in school. Over-zealous blocking based on assumption rather than fact, or online services blocked for questionable reasons.

This can create a paradox; whilst schools want to use more online devices and services, which empower a more effective e-safety education, they are stopped from doing so because of a perception of risk or legality.

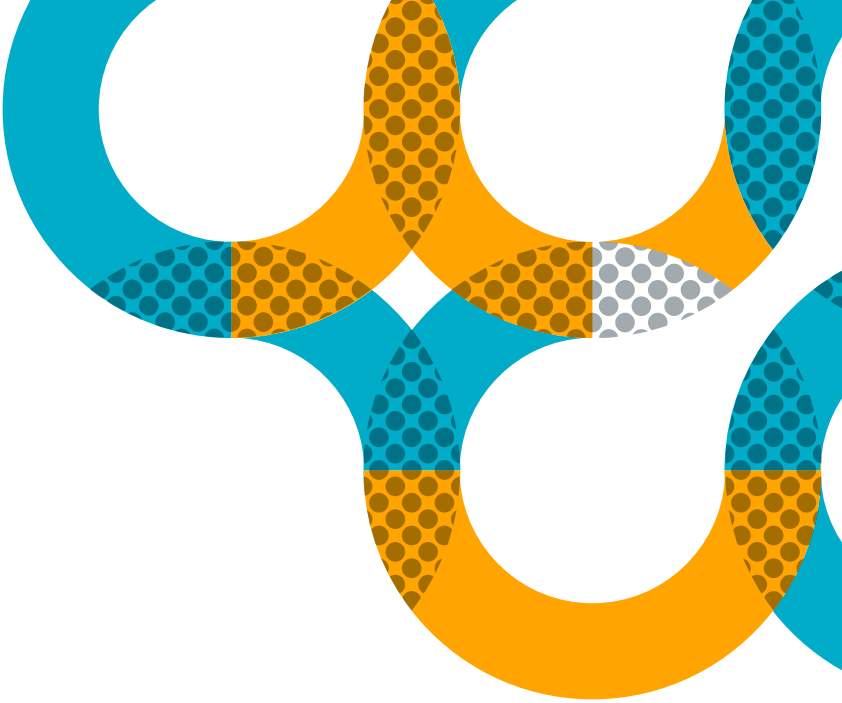
Whilst internet filtering software is a technical tool, it is a tool which is there to provide a safeguarding function: we filter to ensure as much as possible that students and adults are not exposed to illegal or inappropriate websites; we filter to ensure as much as possible that the school has mitigated any risk. But what evidence is there of any inappropriate or illegal activity. One can assume there is a certain amount of inappropriate activity, but what and by whom? Simply blocking this activity does very little without intervening with the source of the behaviour.

The management function of internet filters allows for reports to be created. These reports come in a variety of guises and, if the filter is set up correctly in accordance with the school's Active Directory, they give the evidence that there is (or is not) inappropriate activity from where, when and by whom. But internet filters only give evidence for websites that are being visited.

A much better balance can be achieved by adopting behaviour management (BM) software such as Impero Education Pro. BM software has come a long way over the years, but importantly it monitors all activity on the device (such as sending/receiving emails, opening Word documents and much more), rather than just the internet sites that are being visited. Furthermore the audit trail of evidence is much better suited to a safeguarding need as all "violations" are archived; each violation is a piece of a jigsaw puzzle providing better context to a history of concerning activity.

Whilst BM products these days do provide an internet filtering function, it is still not as comprehensive as a bespoke internet filtering solution. However, with the proper use of both solutions together, a far better balance can be achieved between over-zealous blocking and allowing schools to use the sites and services that they want to use. To understand whether your internet filter is being managed properly you first need to determine what is happening across your internet connection. Is there any evidence of misuse? If so, by who, for what, and what is being done about it?

You may be surprised that there is very little concerning activity, or none at all. But does that mean that sites and services should be blocked "just in case"? Different schools will have different opinions on this; some will be comfortable at this stage to start opening up the filter, some will not be prepared to take the risk, but again this gives us a paradox. Without taking the risk schools will not know if there is a risk, and should there be any inappropriate activity the behaviour element cannot be properly tackled with education and sanctions. In such a situation the adoption



of a more effective solution, such as Impero Education Pro, provides that very balance; the safeguarding assurance that all is or is not well, along with the evidence to appropriately respond to any misuse.

In order to help schools with the significant task of managing e-safety effectively there needs to be a framework in place. This framework gives individual schools flexibility, whilst at the same time promoting standardisation for policy, processes and education. This standardisation is vitally important; it is a benchmark to which schools can monitor their own practices against agreed best practice in order to inform school strategic planning and policy.

In large part, this framework already exists in the form of a freely available online tool from the South West Grid for Learning (SWGfL), otherwise known as the UK Safer Internet Centre (UKSIC). The tool, called the 360 Safe tool, is an online service to which any school can sign up to and input their own data against some set criteria. The output of this is a report that identifies weak or strong areas, along with advice and guidance to bolster the weak areas in order to improve the overall e-safety management within school.

The arguments for and against internet filtering will never go away as they are both arguments with equal strength, however it is my opinion that schools can do far more fairly easily to try and correct the current imbalance of over-zealous filtering. Easily doesn't mean a quick solution; it will take time, but the benefits for school governance, for education, and for safeguarding far outweigh any negatives.

introduction

There can be little argument that the use of technology in education is increasing. This isn't necessarily the use of new hardware (although there has been a significant increase in use of new devices, such as tablets), but also the use of new internet services such as social networking (e.g. blogs, Twitter, YouTube), online storage services such as Dropbox and application services such as Google Docs.

Whilst many schools have the autonomy to enjoy the increased use of such services, many more do not. In large part this is down to a single piece of software and how it is managed – internet content filtering software.

E-safety has become an increasingly important safeguarding matter both at home and at school, with significant pressure on schools to adopt policy and approaches to keep children safe at school and educational approaches to keep children safe outside the school gates. Yet it is also e-safety which is often cited as the reason why some schools cannot use the internet sites or services that they wish to.

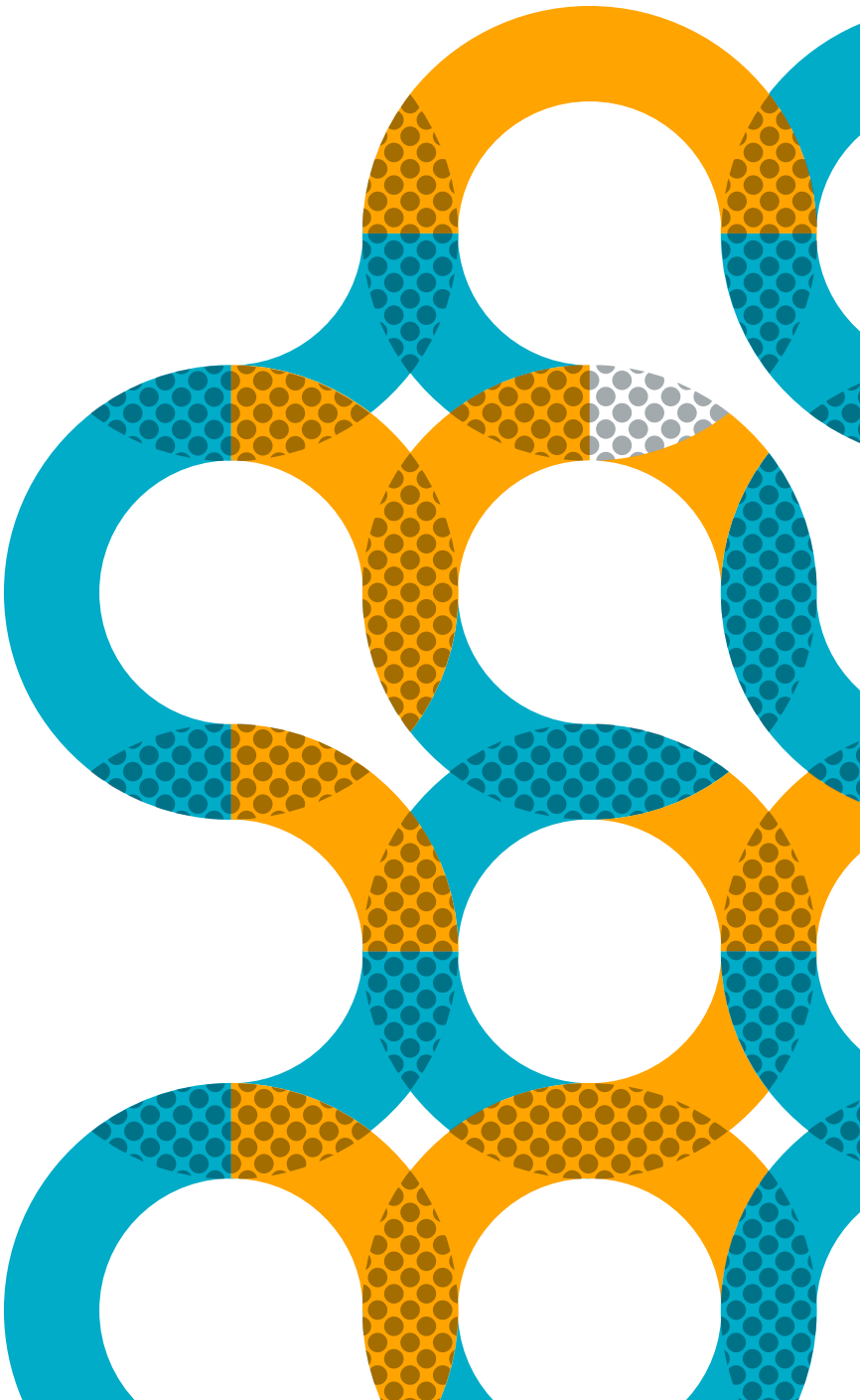
This creates a paradox; schools want to innovate and use more technology and online services with one outcome being a better e-safety education, and yet they may not be able to do so due to over-zealous filtering because of perceived risk.

Is there a balance?

In order to see if a balance can be achieved, it is important to understand a number of things:

1. What is risk?
2. How, in a very general sense, does an internet filter work, and how is it commonly managed?
3. Is there something that does the same thing, but better?

Whilst this paper does not propose a single solution, it looks at whether a better balance can be achieved.



what is risk?

Risk is a vast and complex area, particularly in the online world, and so too are the many factors that create risk or the responses to risk.

In the research paper from Professor Sonia Livingstone, children themselves identify many issues that bother them. It is clear that the very places children go to and use on the internet are the very same places where there is the most risk, whether this is a video sharing site such as YouTube or a social networking site such as Facebook. Regardless of the fact that some of these sites have a lower age restriction, common sense suggests that many children will still use these sites for a variety of reasons. To simply block these sites at home or at school does nothing to empower children to respond to risk.

Age is clearly a factor when it comes to risk and we should remember that children at an increasing early age are using technologies such as tablets and smart phones and are potentially being exposed to risk from a very early age.

For the purpose of this paper risk is simplified to two things:

- Risk to the child or young person;
- Risk to the school.

risk to the child or young person

- **Being exposed to online risk;**
  For example, a child carrying out a simple search in a search engine and being presented with inappropriate or upsetting results; or a young person whose social networking timeline is inundated with unwanted images or violent/distasteful videos.
- **Exposing themselves to online risk;**
  For example a young person continually sharing too much personal information

risk to the school

Potential of liability or reputational risk due to:

- **Doing something that puts the child or young person at risk;**
  For example, loaning a laptop to the child to take home without any appropriate filtering or other safeguarding software installed.
- **Not doing something that puts the child or young person at risk.**
  Poor e-safety education that does not empower the child to understand or respond to risk. Inadequate knowledge or processes to deal with incidents.

filtering software

Internet content filtering is the first line of technical defence in schools. In its most basic form, filtering is the process whereby Internet sites are blocked or allowed against pre-determined categories such as: Adult; Gambling; Advertising; Social Networking and others.

Whilst sometimes seen as one of the more frustrating IT services in schools, internet filtering is one item in the e-safety toolbox that is of particular importance. When talking about an Internet filter there are two aspects:

Broadly speaking

Filtering - this is a pro-active measure to ensure (as much as possible) or prevent users from accessing illegal or inappropriate (by age) websites.

Monitoring - this is a reactive measure and for the most part means searching, browsing or interrogating filter logs (known as the cache) for internet misuse.

Many internet content filters also apply the IWF Black list.

the IWF black (CAIC) list

The IWF is the Internet Watch Foundation, a UK charitable body which has the responsibility for the "notice and takedown" of illegal material either within the UK or worldwide through its partners. The IWF also operates the UK Hotline so that illegal material can be reported by anyone. In this context, illegal material is:

- Child sexual abuse content hosted anywhere in the world.
- Criminally obscene adult content hosted in the UK.
- Non-photographic child sexual abuse images hosted in the UK.

black listing

Within allowed categories of sites there may be individual sites that the school does not wish to be available. These sites may be manually added to a "Black List".

white listing

Within banned categories of sites there may be individual sites that the school wishes to make available, either temporarily or permanently. These individual sites can be added manually to a "White List".

why do we Filter and Monitor?

Schools filter internet activity for two reasons:

- To ensure (as much as possible) that children, young people and adults are not exposed to illegal or inappropriate websites. Inappropriate sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- To ensure (as much as possible) that the school has mitigated any risk to the students, and thereby reduces any liability or reputational risk to the school by making the best possible endeavours to ensure the safety of those students.

We monitor for assurance:

- (As much as possible) that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action or sanctions if necessary.

how are internet filters applied?

Although there are a number of ways, the two most common scenarios are:

1. A filter is procured by contract via the local authority, the local authority grid for learning or other outsourced provider, and is managed centrally. A top-level of filtering categories is applied across users and a degree of management control is sometimes given to schools.

2. An individual school or school cluster procures a filter; all management is taken care of by the school.

Scenario 1 is commonly the most frustrating for schools, particularly if a degree of management is not (or cannot) be given to the individual school (see below).

The degree of management control is largely dependent on the hierarchical technical setup known as the Active Directory. For example, a school hosting and managing its own filter will have all users split into groups within the Active Directory, such as:

- Adults (i.e. teaching staff, support staff);
- Year groups
  - Year 4
    - Class 1
      - User A
      - User B
    - Class 2
      - User A
      - User B
  - Year 5
    - Class 1
      - User A
      - User B

Using such a hierarchy it is possible to apply different internet filtering levels (or categories) down to the individual user level, across the whole school, or both. If the Active Directory is not set up in a way such as above then filtering down to individual user, class, year group is not always possible.

Internet filtering software also has some degree of reporting. For example, you may be able to look up: the total internet sites visited each day (or any other time period); total sites allowed or denied; individual sites allowed or denied; attempted accesses to denied sites by individual users; investigation of internet usage (sites visited or attempts) by individual user.

From a behaviour management perspective the reporting feature is extremely useful. From a safeguarding perspective this reporting feature is the most important, yet least used function.

Whoever is hosting and managing the filter has a very important part to play when it comes to the reporting functionality. Quite often the functionality of the filter is cited as:

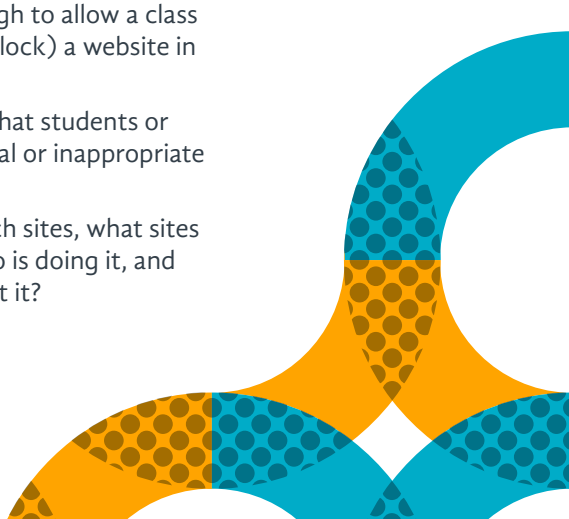
- To prevent users accessing illegal or inappropriate websites;
- To keep students on task;
- To safeguard the child.

But, if the filtering host is not using the reporting functionality on a regular basis:

- How do you know if users are trying to access illegal or inappropriate websites?
- How do you know if they are off task?
- Safeguard the child from what? Safeguarding is an extensive area.

Consider the following:

- Is the filter so locked-down that it is affecting teaching and learning?
- Is the filter flexible enough to allow a class teacher to unblock (or block) a website in class quickly and easily?
- What evidence is there that students or adults are accessing illegal or inappropriate websites?
- If users are accessing such sites, what sites are they, how often, who is doing it, and what is being done about it?



The fact that the reporting functionality within filters is rarely used is understandable:

- There is little context (was the URL input by the user or was it a link from another site?);
- Site URLs are not always obvious, consider http://www.facebook.com against https://www.google.co.uk/search?q=filters&oq=filters&aqs=c hrome..69i57j69i60j0l4.1092j0j7&source id=chrome&espv=210&es_sm=91&ie=UTF-8, which is a simple Google search for the word "filter";
- It can be labour/resource intensive. Dependent on a number of factors such as time-span and number of sites monitored, lines of accessed or denied sites can run into the hundreds of thousands.
- School leaders are not always aware that there is a reporting function, and what that function is capable of.

Let's use a real example to illustrate the above:

School X uses the filtering service offered through the local authority. The LA applies a top-level of blocked sites and categories. These sites and categories can be tailored with a simple call to the Helpdesk, but the LA also makes available a management console so that individual schools can take their own responsibility and manage the filter themselves. In the secondary schools it is mainly the in-house technical teams that manage the filters, but the primary schools tend to leave the management up to the LA.

During a monthly filtering audit at the LA there is an alarming find. A KS3 student has been attempting to access some sites which, by the web title, could be illegal. A quick phone call to the Headteacher reveals the school was not aware of this very serious safeguarding matter. Established Safeguarding Children's Board processes begin.

This very simple example raises some questions:

1. Whose responsibility is it to manage the filters? In this context, management includes the regular investigation of filtering activity using reports. Is it the responsibility of the school, the LA, or a joint responsibility?
2. Within a secondary school (and some primary schools) the management responsibility is devolved to a technical team, yet an internet filter is a safeguarding tool. One could argue that the technical team has responsibility for the running and functionality of the tool, but should the technical team have responsibility of the usage? At the very least, should senior management have visibility of regular reports, so that appropriate educational and safeguarding decisions can be made?

behaviour management software

Behaviour management (BM) software is fundamentally different to content filtering software. Whereas filters allow or deny access to websites, BM software uses categories, such as lists of words or phrases, to capture and identify inappropriate activity on PCs, laptops, and increasingly other devices. Once captured, a screenshot is taken and forwarded to a particular person in the school along with other identifying features such as: screenshot identifying the word or phrase causing concern; logged in user; IP address; time etc.

BM software is also very different, as it is not just monitoring websites that have been visited, but any activity on the device. For example, that could be typing or receiving an email, a Word document, a chat session, or anything else that is text based.

Over the last few years, BM software has come a long way; no longer is it just a piece of software that monitors words or phrases. Products such as Impero Education Pro is a fully integrated toolbox giving behaviour, classroom and device management across PCs, laptops and smart devices, such as iPads. BM software invariably comes with an embedded internet content filter, although in my experience the filtering element is not as comprehensive as a bespoke filtering solution.

There are two huge advantages to using BM software over a dedicated internet filter:

1. Incidents are reported to a person straight away along with the evidence.

2. All incidents are archived; this is very important. For example, a school may have a concern about a particular child. All the incidents for that child can be viewed from the archive, thereby giving greater context. This is a jigsaw effect; one incident alone may not be enough to highlight a concern, but a number of incidents provides a bigger, more complete picture.

is there a case to remove internet filtering in schools?

There is no straightforward answer to this. The opposing yes and no camps both have strong and valid viewpoints, some of those being:

no

- There are too many risks to children and young people(CYP) on the internet.
- The filter is in place to protect children from harmful (e.g. pornographic) material.
- There is a risk of liability to the school if children are exposed to inappropriate or harmful material.
- We cannot take the risk that children or adults can access illegal material.

yes

- In order to understand risk, CYP should be gradually exposed risk. This is an issue of behaviour, not technology; behaviour needs to be managed.
- Children will have free reign at home, whether on the PC or their mobile phone (although this will change in 2014 with the Government strategy to have an internet filter across every home broadband connection). Protection is having the knowledge to mitigate and/or respond to risk.
- The school, as the corporate parent, has a duty to protect the child, however that doesn't mean wrapping in cotton wool but, rather, educating and building resilience.
- The majority of ISPs already block illegal material using the IWF Black (CAIC) list.

In an online context, the fundamental life-skills a child must learn from an early age would include:

- **Resilience** – for example, understanding that comments can be taken out of context.
- **Empathy** – just because you can't always see emotion online doesn't mean there isn't any emotion. The lack of visual emotion is not an excuse for dis-inhibition.
- **Risk assessment** – there are many risks online as there are in the real world. Users have to understand these risks and how to mitigate and minimise or respond to risk.
- **Critical thinking** – as in real-life, not everything is as seen. Anybody can put or say anything on the internet. Children need to understand and build the capacity to distinguish what/who can be trusted, and those that can't.

The internet is a resource to enhance teaching and learning, yet can be a frustration due to over-zealous blocking. Arguably, the case against removing an internet filter in schools will always win. Schools would be very nervous about doing something that potentially opens up the child, adult or the school to risk. However, is it possible to achieve a balance whereby the filter can be less restrictive?

If there is such a thing, the balance is dependent upon the individual school leadership team rather than a one-size-fits-all balance. Therefore any solution has to:

- Allow sufficient flexibility to be tailored to the individual, the class, year group and school.
- Be easy (non-technical) to use.
- Allow flexibility to allow the class teacher to use professional discretion within agreed school boundaries and established policy.
- Support reporting mechanisms that allow reporting to the school pastoral care and senior management.

	internet filter	behaviour management
Embedded filter?	Yes	Yes
Can be tailored to age?	Yes - dependent on school AD configuration	Yes - dependent on school AD configuration
Includes monitoring functions?	Yes, internet access only	Yes, all device activity
Includes reporting function?	Yes, internet activity only	Yes, all screen activity, not just internet access.
Reports concerning activity to member of staff?	No	Yes, to one or more members of staff immediately or archived for later viewing.
Can enforce school e-safety policy and AUP?	Yes, limited	Yes, granular level of capture/report provides tangible evidence.
Managed by teachers or pastoral care?	Rarely	Commonly

*Note: the table above is very generalised; different filtering and BM solutions will have different functionality.

One may determine from the above table that the range of functionality within a BM solution is far more than that of a bespoke web filter. The range of features can be tailored to meet the school requirement relatively easily but with the added over-arching requirement that inappropriate activity is monitored and reported to the correct person.

can a balance be achieved?

Any balance is a matter of individual (school) interpretation. To be able to answer the question, the individual school must have all the facts, such as:

- Who manages your filter?
- Are reports made available to you, or do you know what types of reports can be made available?
- What categories are currently allowed or denied via the internet filter?
- Through the reports, is there any evidence of inappropriate (or attempted inappropriate) use?
- If so, what and by whom?
- Do members of staff and the students believe that the current level of filtering is overly-restrictive based on their experience in the classroom?

In order to achieve a balance, you first of all need to determine how the balance is currently weighted. Without understanding how your filter works (in a non-technical sense) or is managed, without knowing if there is a worrying amount of access to or attempt to access) inappropriate sites, a balance is very difficult to determine.

Becta PIES model

Even if a school is confident to have more balanced internet content, the lack of any national standardisation will still raise concerns with many. Standardisation allows for comparison of best practice so that a school that is more confident in what it is doing can take the lead and help other less confident schools.

However, there needs to be a number of elements to that standardisation. In 2005, Becta introduced the PIES model

'Becta's PIES model is an effective framework for approaching safeguarding strategy across learning provision. It offers a simple way of mitigating against risks through a combination of effective policies and practice, a robust and secure technology infrastructure, and education and training for learners and employees alike, underpinned by standards and inspection'.

Becta, Safeguarding in a Digital World, April 2010

This model was a framework to strategically manage e-safety in school. However, in 2005 the technology (in terms of the hardware and the online services) in use within schools and at home was very different to what it is in 2014. The social aspect of the internet can shape children's online experiences; it also changes the scope to exposure to online risk .

Mobile technologies such as tablets and smart phones plus internet services such as social networking (including blogging), amongst many other online services and initiatives, were relatively unheard of in an educational context. One-to-one device schemes; bring-your-own-device (BYOD) initiatives; anytime-anywhere learning; online application services such as Evernote, Dropbox, Google Apps etc. has completely transformed the landscape. Furthermore, recent additions and changes to Ofsted inspections and the national curriculum (Computing) have determined what schools must do in regards to inspection and education.

is PIES still relevant?

Does the PIES model still give us this standardisation, or framework, that is:

a) Still usable today?

b) Standardised?

c) Flexible enough to meet the needs of individual schools now and in the future?

d) A useful baseline and comparison of best practice?

With a bit of tweaking and updating, the answer is yes. In particular this is because of the Ofsted e-safety inspection framework (from Sep 2012) and the introduction of e-safety into the national curriculum (from Sep 2014), which now stipulates the Standards and Inspection element.

Whilst this paper concentrates on the infrastructure element, the Policies and Practice, and Education and Training elements in regards to Ofsted and the national curriculum are given in Annex A and B respectively for completeness.

PIES - infrastructure

PIES definition:

- Technological tools used effectively to manage and monitor the use of ICT provision. In addition to education and policy, organisations will want to explore how tools can be used effectively to filter content, and to track and manage use of systems, software and internet access.

Ofsted requirement:

- Recognised Internet Service Provider or RBC (Regional Broadband Consortium) together with age-related filtering that is actively monitored.

In addition, the monitoring and evaluation aspect requires:

- Risk assessment taken seriously and used to good effect in promoting e-safety.
- Using data effectively to assess the impact of e-safety practice and how this informs strategy.

Whilst internet filtering alone can be used for some of the elements above, it is not an easy task, particularly for a school with no in-house team (e.g. primary school), and even more so if the filter is provisioned via a local authority, regional broadband consortium (learning grid) or other outsourced provider.

Unless the granularity of management and control is within the remit of the individual school, all of the elements of the above are not easily achieved. However, using a service such as Impero Education Pro, all of the above can be achieved.

- **Manage and monitor** – All devices within the school managed in relation to;
  - Behaviour, which is captured, archived and forwarded;
  - Software and licensing for legal compliance;
  - Much more including print, power and patch management.
- **Age-related filtering that is monitored** –
  - All users defined within groups (e.g. class or year groups) and monitored as above.
- **Risk assessment** – carried out according to the technology and services used within (and outside) the school. Mitigation put in place and embedded within the e-safety (and acceptable use) policies. Monitoring and compliance as above.
- **Use of data to assess impact of practice** – internet filtering reports do not give the whole picture in any context. However, archived data (captures and violations) from Impero Education Pro is used to assess the impact of the school e-safety policy down to the individual user.

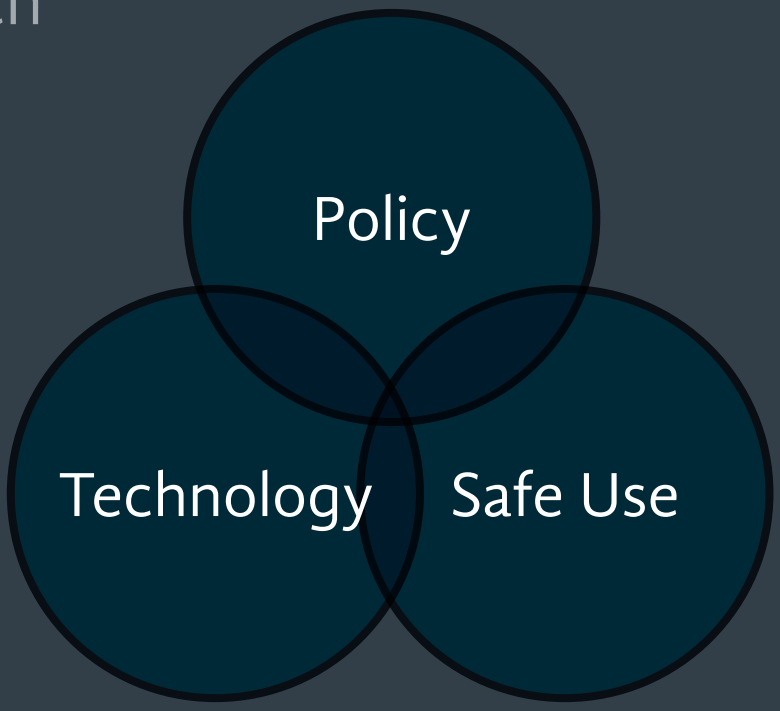
a framework approach

As previously mentioned in this report, it is questionable whether there is a one-size-fits-all solution. Rather, a framework approach that gives standardisation, clarity and advice would be better suited in order that individual schools can make their own decisions, which is modelled against evidence and best practice.

what would this framework look like?

Very much like Becta PIES, it comes down to the three most important areas: policy; technology; safe use. Each area would stipulate the minimum standards expected, but importantly how to achieve those standards with examples of best practice. It should take into account all the needs and requirements of the Ofsted inspection and the national curriculum, but also be flexible enough to respond to other unknown risks.

- **Policy** – clear, concise, robust policies in place that:
  - set the boundaries of appropriate use of technology in your school;
  - ensure that all users are aware of their responsibilities;
  - clear processes to respond to any incidents of risk or behaviour.
- **Technology** – this is not the technology that is used in school, but the technology that is used to safeguard, for example internet filtering and behaviour management software.
- **Safe use** – empowering all users with the knowledge to identify and respond to risk; to create a positive digital footprint and use the internet and technology with respect; positive safe-use messages in order to enjoy technology, safely.



Is there something currently that can be used or developed further?

Yes. For a number of years, the South West Grid for Learning (UK Safer Internet Centre) has made available a free tool called the 360 Safe tool . This is a self-review tool that encompasses all of the requirements of Policy, Technology and Safe Use, whilst giving clear direction and advice at the same time.

Importantly the tool also uses comparative data from schools that have already used it and also gives a threshold for each area. Therefore, you can see if you are meeting or falling below expected standards.

Of course, it is the application of the tool, rather than the tool itself, that is important. By using 360 Safe you are presented with clear indications of where improvement is needed, and it is this very information that can feed into the school strategic plan.

summary

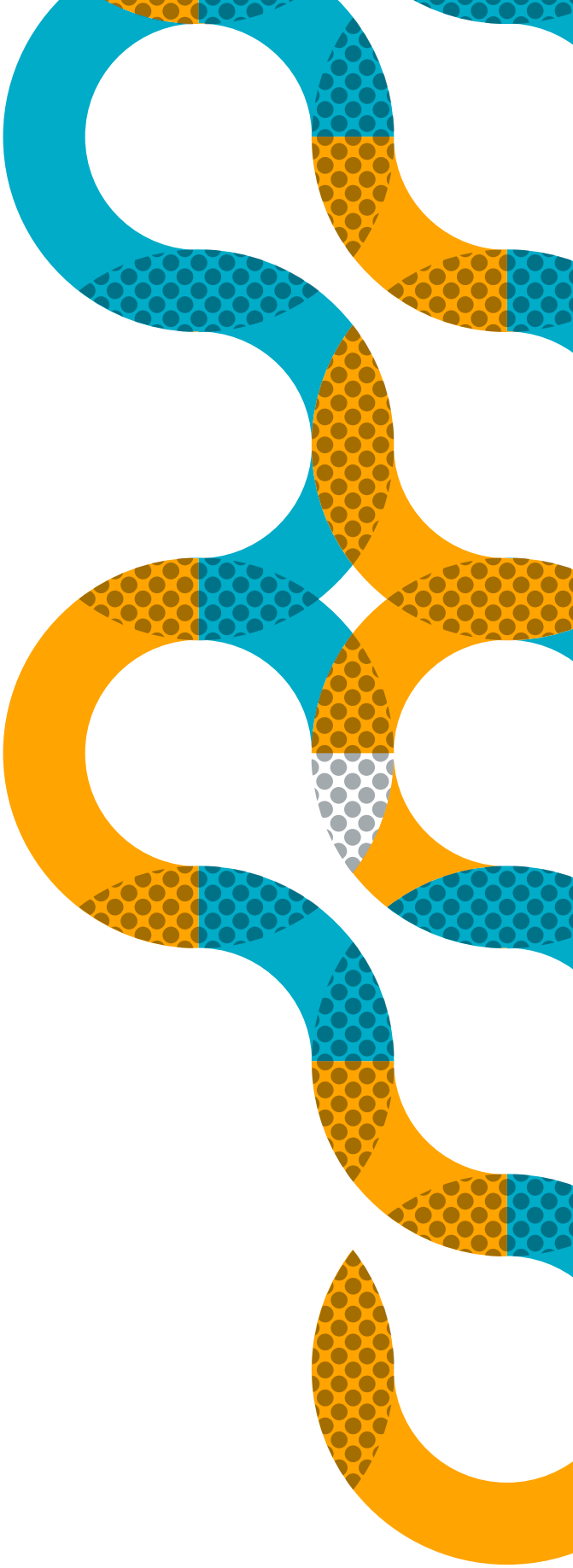
E-safety is a vast and increasingly important area, particularly for schools who need to move away from “doing” e-safety to “managing” e-safety.

Managing e-safety is about having the right tools, the right processes and empowering the right information. Importantly, those areas also need to be evidence based.

The arguments for and against internet filtering will never go away. In my own opinion, I don’t believe a school can ever do without a filter, however I do feel that filters can be managed far more effectively than they currently are, in order to reduce the amount of over-zealous blocking by providing facts (through reports) that there is, or is not, evidence of inappropriate activity. Much of the over-zealous filtering is down to assumption or ignorance rather than fact, and this will continue to cause issues as more and more schools wish to use more ICT and services to innovate and enhance teaching and learning.

With that said, the evidence that can be exported from many filters is still difficult and time-consuming for many schools, however far more appropriate balance can be achieved with the adoption of behaviour management software such as Impero Education Pro which can provide tangible, contextualised evidence.

Of course, the usefulness of tools such as filters and behaviour management solutions are questionable if they are not adopted into a whole-school approach. Remembering that although these are technical tools, they are in place to support schools statutory safeguarding requirement, and are therefore one piece of a larger jigsaw. The adoption of a framework approach to managing e-safety would provide schools with: standardisation; consistency; flexibility; guidance and best practice.



annex A – Ofsted e-safety inspection framework

Within the framework there are 8 areas that need to be considered in depth:

whole school consistent approach

- High quality leadership and management make e-safety a priority across all areas of the school.
- All teaching and non-teaching staff can recognise and are aware of e-safety issues.
- A high priority given to training in e-safety, extending expertise widely and building internal capacity.
- The contribution of pupils, parents and the wider school community is valued and integrated.

E-safety is safeguarding, not technology. All members of staff (not just teaching staff) have a responsibility to all children and to each other. Because of the potential of serious risk to both students and staff, it is important that there is a good level of understanding of these risks, not only in terms of how to deal with the risks but also how to recognise the risks.

The thoughts and opinions of children and their parents are a vital element in order to feed school strategy and policy.

robust and integrated reporting routines

- School-based reporting routes that are clearly understood and used by the whole school, for example online anonymous reporting systems.
- Report Abuse buttons, for example CEOP. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support.

staff

- All teaching and non-teaching staff receive regular and up-to-date training. One or more members of staff have a higher level of expertise and clearly defined responsibilities.

Training should be specific to the audience. For example, training for the senior leadership team and governing body will differ from "all staff" training. Staff will receive a comprehensive overview of the latest risks and behaviours, the technology that young people are using, processes and procedures for responding to incidents etc. Training for SLT and the governing body will expand on staff training to further consider the school context, e.g. effective risk assessing, mitigation, ensuring there are no risks to the children, to the staff, and reducing any liabilities to the school.

policies

- Rigorous e-safety policies and procedures are in place, contributed to by the whole school, updated regularly and ratified by governors.

Policies wrap-up school governance in areas such as: how technology is used in the school; boundaries of appropriate and inappropriate use; processes and flowcharts for responding to incidents. Policies must be clear and concise as they must also be signed as read and understood by all, including children (if age appropriate).

education

- An age-appropriate e-safety curriculum that is flexible, relevant and engages pupils' interest; that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm, and how to take responsibility for their own and others' safety.

e-safety is a life skill and, as such, it is not something that is taught in a single lesson or an assembly. The most effective way is to embed positive, safe use messages within an established curriculum.

infrastructure

- Recognised Internet Service Provider or RBC (Regional Broadband Consortium) together with age-related related filtering that is actively monitored.

Broadband is available from dozens of different companies at varying price and quality levels. Historically, schools have received their broadband provision through a regional broadband consortium via the local authority. There are many reasons for this, but the main reasons are value for money, security and end-to-end management.

Filtering should be managed, not a tool for blocking. It is important that filtering is configured to be age-appropriate. The most common configuration is different policies set for each key stage, and a separate policy for adults.

monitoring and evaluation

- Risk assessment taken seriously and used to good effect in promoting e-safety.
- Using data effectively to assess the impact of e-safety practice and how this informs strategy.

management of personal data

- The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998.

Impact Levels (IL) are categorised as either 1, 2, 3 or 4. There are higher, however they do not relate to schools. Generally speaking, the Impact Levels are as follows:

IL1 – General information
IL2 – Learning platforms or portals; general student data
IL3 – SEN, school MIS, health records
IL4 – Looked after children

recommendations

The inspection framework also gives a number of recommendations that all schools should understand:

- Audit the training needs of all staff, provide training to improve knowledge and expertise in the safe and appropriate use of new technologies.
- Work closely with all families to help them ensure that their children use new technologies safely and responsibly, both at home and at school.
- Use pupils' and families' views more often to develop e-safety strategies.
- Manage the transition from locked down systems to more managed systems, to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school.
- Provide an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies.
- Work with their partners and other providers to ensure that pupils who receive part of their education away from school are e-safe.
- Systematically review and develop their e-safety procedures, including training, to ensure that they have a positive impact on pupils' knowledge and understanding.

annex B – e-safety in the National (Computing) Curriculum

(From Sept 2014)

Every state-funded school must offer a curriculum which is balanced and broadly based and which:

- Promotes the spiritual, moral, cultural, mental and physical development of pupils at the school and of society, and
- Prepares pupils at the school for the opportunities, responsibilities and experiences of later life.

All schools should make provision for personal, social, health and economic education (PSHE), drawing on good practice. Schools are also free to include other subjects or topics of their choice in planning and designing their own programme of education.

A high-quality citizenship education helps to provide pupils with knowledge, skills and understanding to prepare them to play a full and active part in society.

It also ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world, who are responsible, competent, confident and creative users of information and communication technology.

key stage 1

Use technology safely and respectfully, keeping personal information private; know where to go for help and support when they have concerns about material on the internet

key stage 2

Understand computer networks including the internet; how they can provide multiple services, such as the world-wide web; and the opportunities they offer for communication and collaboration.

Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

Use technology safely, respectfully and responsibly; know a range of ways to report concerns and inappropriate behaviour

key stage 3

Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct and know how to report concerns.

key stage 4

Understand how changes in technology affect safety, including new ways to protect their online privacy and identity, and how to report concerns.

acknowledgements and references

Livingstone, Sonia and Kirwil, Lucyna and Ponte, Cristina and Staksrud, Elisabeth (2013) In their own words: what bothers children online? with the EU Kids Online Network. EU Kids Online,

London School of Economics & Political Science, London, UK.

http://eprints.lse.ac.uk/48357/

Holloway,D., Green, L. and Livingstone, S. (2013). Zero to eight. Young children and their internet use. LSE, London: EU Kids Online.

http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf

Internet Watch Foundation – http://www.iwf.org.uk

British Educational Communications and Technology Agency. A non-departmental public body funded by the DfE pre-2011 when government funding was cut.

Archived explanation of PIES model - http://archive.excellencegateway.org.uk/page.aspx?o=197297

Mascheroni, Giovanna, Ólafsson, Kjartan, (with Cuman, Andrea, Dinh, Thuy, Haddon, Leslie, Jørgensen, Heidi, Livingstone, Sonia, O'Neill, Brian, Ponte, Cristina, Stald, Gitte, Velicu, Anca and Vincent, Jane) Mobile internet access and use among European children: initial findings of the Net Children Go Mobile project. Net Children Go Mobile project report, (Milan, Italy: Educatt, 2013)

http://eprints.lse.ac.uk/54244/

Ofsted, December 2013, Briefings and Information for use during inspection of maintained schools and academies - http://www.ofsted.gov.uk/resources/briefings-and-information-for-use-during-inspections-of-maintained-schools-and-academies

National Curriculum for Computing (from Sept 2014) - https://www.gov.uk/government/collections/national-curriculum

South West Grid for Learning (UKSIC) e-safety www Self Review Tool

http://www.360safe.org.uk/