UK Schools Online Safety Policy and Practice Assessment 2016

Prepared By Prof Andy Phippen for SWGfL, October 2016

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter, EX2 5WS
Registered in England and Wales, Company Number 5589479. Charity Number 1120354. VAT Reg. Number 880 8618 88

Annual Analysis of 360 degree safe self-review data

Exec Summary

This analysis of data from the 360 degree safe tool draws from the self-review data of over 8000 schools across the country to consider the "state of the nation" related to online safety policy and practice. This sixth annual analysis shows, in general, an improving picture compared to previous years, with the data demonstrating increases in performance against 28 aspects related to online safety in schools. Similarly to previous years, strengths lie in policy and technical infrastructure, and weakness around training, evaluation and community engagement:

Areas of strength are:

- effective connectivity and filtering in place (Almost 65% of schools have excellent or good connectivity and filtering in place);
- the scope of online safety covered in school policies (Almost 70% of schools have strong online safety policies in place);
- effective Acceptable Usage Agreements in place (Almost 55% have a detailed and effective Acceptable Usage Agreement in place);
- policy addressing issues around digital images and video;
- effective online safety policy in place (Only 15% of schools have nothing in practice around policy development).

Areas of weaker practice are:

- effective engagement with the wider school community on issues related to online safety (almost 60% of schools have no engagement with the community on online safety issues);
- the evaluation mechanisms in place to measure the impact of online safety policy and practice in schools (over 50% of schools have no means to evaluate the impact of their online safety strategy);
- the effectiveness of training for school governors related to online safety (55% have carried out no governor training around online safety issues);
- the effectiveness of training for staff on matters related to online safety (Almost 50% have no staff training to date around online safety);

- Almost 35% have no data protection policy in place, even though they are legally responsible for secure storage and management of sensitive personal data about children and young people

Areas of technical security (Technical Security, Filtering and Monitoring, Password Security) are stronger in secondary schools than Primary schools. Password security varies considerably between Secondary and Primary schools and whilst this might be expected, given the generally lesser technical resource available in primary schools, passwords are a critical component in managing sensitive data and device access.

The starting point for newly registered schools is weaker than early adopters of the tool when the profiles of those schools registered in 2016 are compared with the overall averages across all aspects.

Over 50% of both primary and secondary schools have reported there is no governor training around online safety.

The data suggests that data protection compliance is emerging as an issue for at least 1 in 3 schools.

Contents

1. Introduction

360 degree safe (https://360safe.org.uk/) was launched by SWGfL in November 2009 to allow schools to evaluate their own online safety provision; benchmark that provision against others; identify and prioritise areas for improvement and find advice and support to move forward. 10,000 schools now use the free resource which integrates online safety into school policy and the curriculum in a way that actively challenges teachers and managers in the school to think about their online safety provision, and its continual evolution.

The flexibility of 360 degree safe is such that it can be introduced at any speed (as appropriate to the school's situation) and can be used in any size or type of school. As each question is raised so it provides suggestions for improvements and also makes suggestions for possible sources of evidence which can be used to support judgements and be offered to inspectors when required.

In one particularly interesting development, where evidence is needed, the program provides links to specific areas of relevant documents, rather than simply signposting documents on the web. This saves time for everyone concerned about online safety, and allows the school to show immediately the coverage and relevance of its online safety provision.

360 degree safe will also provide summary reports of progression, (again this is useful when challenged), and is an excellent way of helping all staff (not just those charged with the job of implementing an online safety policy) to understand the scope of online safety and what the school is doing about the issue.

Above all 360 degree safe provides a prioritised action plan, suggesting not just what needs to be done, but also in what order it needs to be done. This is a vital bonus for teachers and managers who approach the issue of online safety for the first time, in a school which has no (or only a very rudimentary) policy.

This self-review process is more meaningful if it includes the perceptions and views of all stakeholders. As broad a group of people as possible should be involved to ensure the ownership of online safety is widespread.

Once they have registered to take part in 360 degree safe process the school will be able to download the Commitment to E-Safety Certificate for signing by the Headteacher (and

Chair of Governors) as a sign of the commitment to use the online tool. Once the school has completed some of the elements of 360 degree safe tool then the E-Safety Certificate of Progress can be awarded. When the school meets the benchmark levels it is formally assessed via inspection before being awarded the "E-Safety Mark", an award validated and approved by Plymouth University. Samples from E-Safety Mark inspections are used throughout the report to illustrate examples of best practice across different aspects to the illustrate the relationship between the overall analysis of the national data and the impact the tool can have on the staff and pupils in schools across the country.

In September 2010, the first analysis of the 360 degree safe database was published by South West Grid for Learning (https://360safe.org.uk/About-the-Tool/Content/News-Articles/360-degree-safe-Largest-ever-survey-of-E-Safety-i) based upon data returned from 547 establishments across England. The tool has grown from this point and this year the analysis collects data from over 8000 educational establishments across England.

2. Methodology

The tool defines 28 aspects related to online safety, from policy issues (Acceptable Usage Policy, policy on mobiles, etc.) through factors such as staff training to technical measures like filtering[1]. For each aspect the tool provides a numeric rating between 1 (the strongest rating) and 5 (the weakest) with a detailed definition for each to allow schools to determine, for each aspect, how their school performs. Generally, these levels are defined as:

Table 0-1 - Overall level definitions for the 360 degree safe tool

Level 5	There is little or nothing in place
Level 4	Policy and practice is being developed
Level 3	Basic e-Safety policy and practice is in place
Level 2	Policy and practice is coherent and embedded
Level 1	Policy and practice is aspirational and innovative

[1] An overview of the 360 structure, detailing aspects covered, can be found at https://360safe.org.uk/Files/Documents/360-degree-safe-Structure-Map.

Schools conduct a review of their establishment against these criteria, for each one deciding at what level they currently perform (which each level descriptor very clearly defined within the tool). Every submission to the tool is recorded into a database to to initially baseline the schools practice. However, the retains previous submissions and will allow the school to define a development plan to move their online safety policy and practice on and it is intended to be used as (and frequently is used as) a school improvement plan. The storage of all data in a comprehensive database, however, provide a large dataset for analysis of online safety policy and practice across the educational landscape as a whole.

Analysis of the data focuses on establishment's self-review of their online safety policy and practice, exploring their ratings against the 28 aspects of 360 degree safe. Aspect exploration allows the measurement of degrees of progression and improvement in the self-review and those where, in general, policy and practice among UK educational establishment requires support to deliver further progress. The tool allows both overall analysis of aspect performance across the whole dataset, as well as being able to focus on specific aspects, regions, times, etc. The dataset is unique in the world of online safety – which provide use with an peerless opportunity to explore data submitted by schools themselves across the country to get a national perspective.

It is acknowledged that the data being explored is self-reviewed – the establishments give themselves ratings against the aspects and level definitions. It is not "validated" data without an inspection, which will only occur if the establishment wishes to gain accreditation. However, self-review is well established practice within the UK school system and level descriptors are very clearly defined. In addition, accreditation visits to date have demonstrated that in the instances of inspection that have occurred, self-review ratings have been generally accurate. Indeed, many schools are generally conservative with their assessments. We also now have a sufficiently large database that "anomalous" returns are very apparent and can be followed up with the school or its local authority.

A further validation comes from being able to compare data against previous years analysis (this is the 6th annual analysis of the 360 degree safe database). As will be demonstrated below, the "shape" of the data is consistent, even with the addition of numerous new establishment. This implies a highly normalized dataset where submission of the self-review data is consistent across establishments. One final measure of validity is that the tool does have an aspect of external validation – schools may opt for online safety certification when they reach a certain level on the tool. If a school wishes to apply for certification, they are

subject to a daylong inspection which qualitatively judges the quality of their online safety provision and policy and allows judgment to be made on their self review scores. To date this mechanism has not identified any anomalous scores – schools are generally consistent and honest with their ratings. It might be argued that, given the tool is intended for development and improvement purposes, it is not in the school's interest to inflate their scores.

3. Details of the Establishments Analysed

The previous year's analysis was published in October 2015[2]. Data for this year was collected mid November 2016, so presented here is an analysis based upon slightly more than 13 months of progression from the previous report. The dataset for the tool is a "living database" in that it is constantly in use with new data being added. Therefore we have to take snapshots of the database as a whole for analysis. It should also be noted that the tool allows schools to perform the self-review at their own pace, it is not necessary for them to complete 28 aspects immediately. Therefore, we will have a difference between the number of schools who have registered, the number who have embarked upon the review, and the number who have completed it. Table 2 shows the basic statistics for establishment registrations at this time:

Table 0-1 - Database baseline figures in November 2016

Establishments signed up to the tool on November 2016	8238[3]
Establishments who have embarked on the self-review process	6620
Establishments with full profiles completed	3005

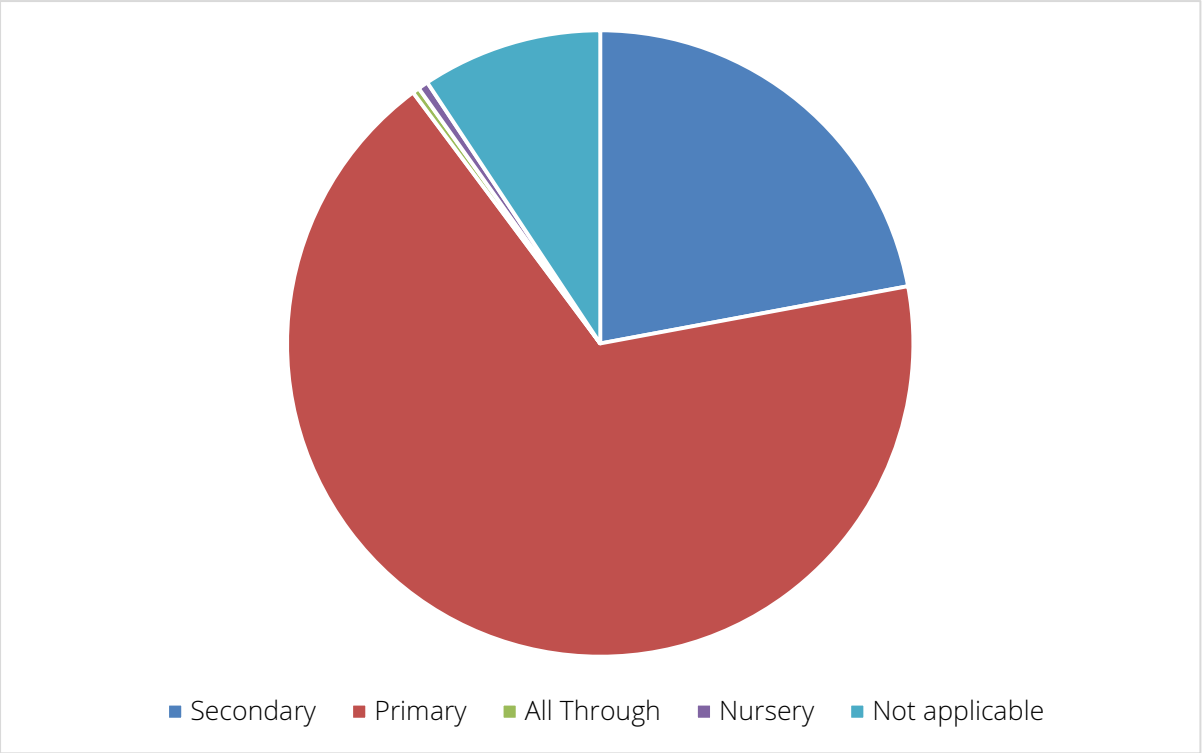
We can also consider the establishments registered in terms of phase, as shown in figure 2. Unsurprisingly there is mainly a split between primary and secondary schools, with the majority being primaries (which we would expect given the higher proportion of primary schools compared to secondary schools) There are also a number of "not applicable" establishments that have been omitted from this graph as they are not "typical" school settings (for example, local authorities, pupil referral units, community special schools, independents, etc.). While analysis of these atypical settings may be conducted in the future

[2] UK Schools Online Safety Policy and Practice Assessment 2015 Annual Analysis of 360 degree safe self
Review data , Phippen A, http://swgfl.org.uk/news/Files/Documents/Online-Safety-Services/360-Report-2015-Online-Safety-Policy-and-Practice.aspx

[3] In total if we incorporate registrations from 360 Scotland and 360Cymru there are over 10500 schools signed up to use the tool in the UK

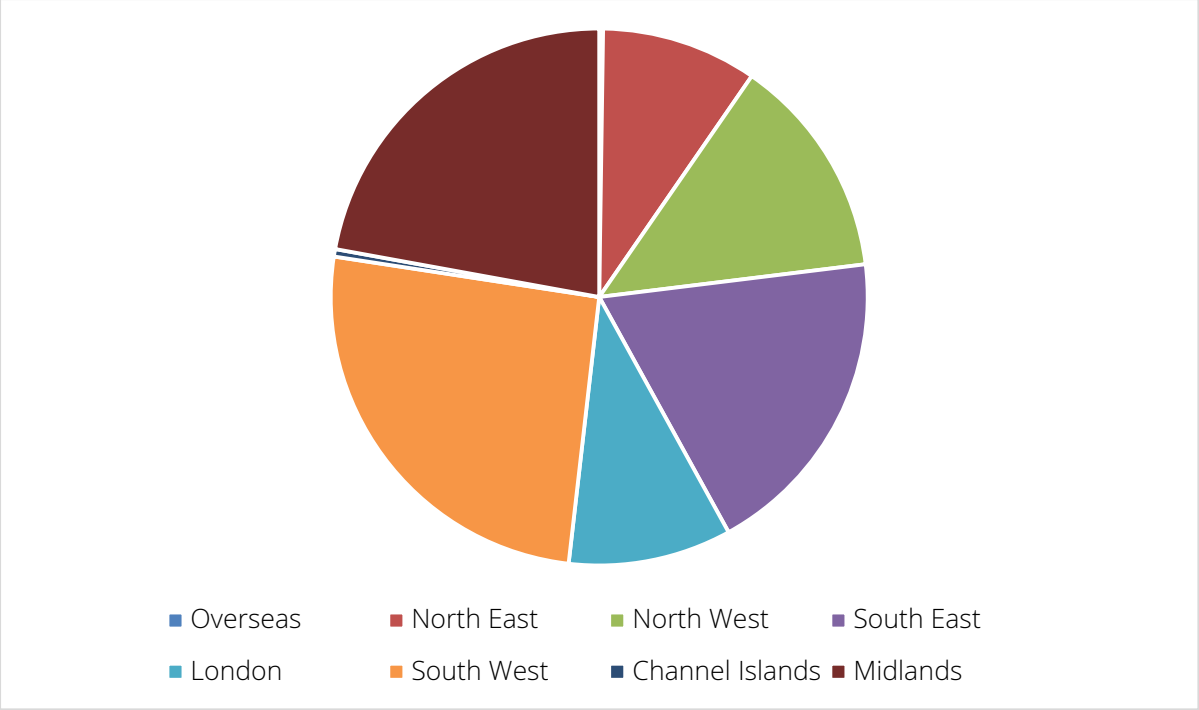
(particularly related to independent schools) the focus of this report lies squarely with primary and secondary phases.

Figure 0-1 - Establishment phase



In terms of regional distribution, the roots of the tool lie in the South West, and we can still see that this region still have more schools using the tool than in other regions. However, as shown in figure 3-2, there is now a broad geographical spread across the whole country. While regionality is something we have explored in past reports, this is not going to be explored in this year's analysis, primarily because we see little difference in the performance of schools in different regions. This report focuses on England and Northern Ireland; it does not include data from 360Cymru or 360Scotland.

Figure 0-2 - Location of establishments



4. Activity on 360 degree safe

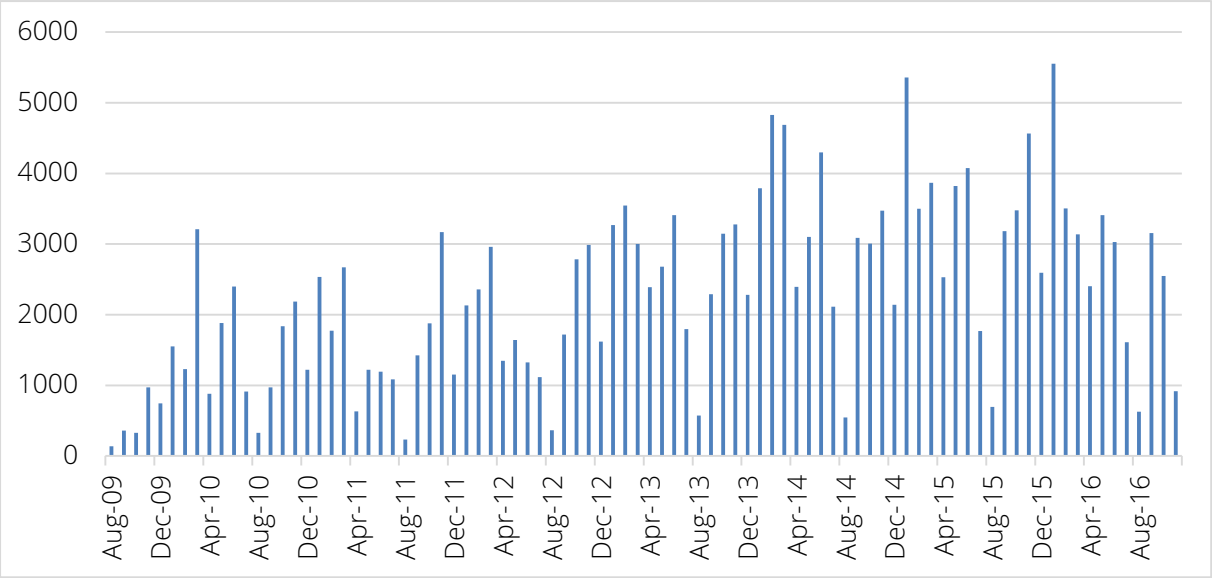
While section 3 explores the basic statistics around the number, location and phase of schools using the tool, this section goes into far more detail about the tool's use and the implications of such in terms of grassroots activity and also educational policy nationally. The tool and its data provide us with a unique insight into online safety policy and practice in schools based upon an unparalleled sample size. We are in a position not to say "we think" this is going on in schools but that "we know" this to be the case.

An interesting piece of analysis, which allows us to view activity on the tool across the school year, is illustrated in figure 4-1. This figure shows the number of times any establishment registered to use the tool has made a change on their school data – it presents us with an interesting measure of how online safety is being tackled in schools.

We can see clear pattern of activity in each school year, with peaks in activity when at the start of the academic year and also after the Christmas break. The spring term, in particular, seems to be the time where there is a lot of activity on the tool. As reported upon in previous analyses the impact of national policy change can be seen in the tool data. In September 2012 OFSTED included references to online safety within their Inspection Handbook for the first time and we saw a major increase in activity on the tool in this time.

Revisions to Ofsted inspections and the update to Keeping Children Safe in Education 2016 (England) continue to drive engagement with the tool.

Figure 0-1 - Activity per month



In figure 4-1 we can see that while the shape of the 2014-15 and 2015-16 cycle is very similar, we do not see a large increase in activity over the last year, even though there have been a significant number of new registrants on the tool. Comparing ratings per month (Figure 4-2), we can see a profile shift in use of the tool towards the first 6 months of the academic year. This may be more in line with typical school improvement cycles

Figure 0-2 – Ratings per month

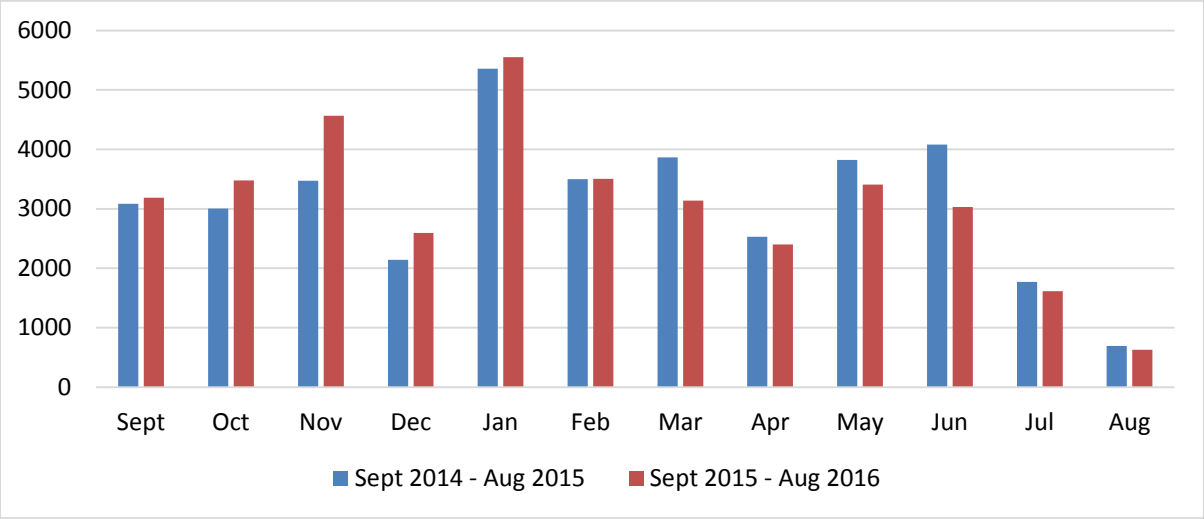
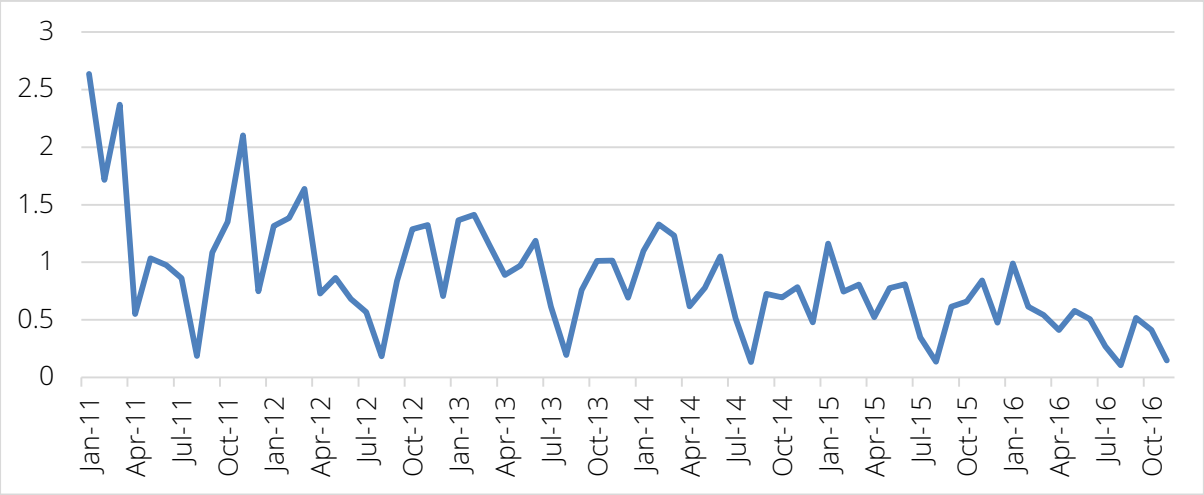


Figure 0-3 – Activity/Registrations. Comparing activity with number of establishments



In figure 4-3, the can see the rate of activity based upon registrants

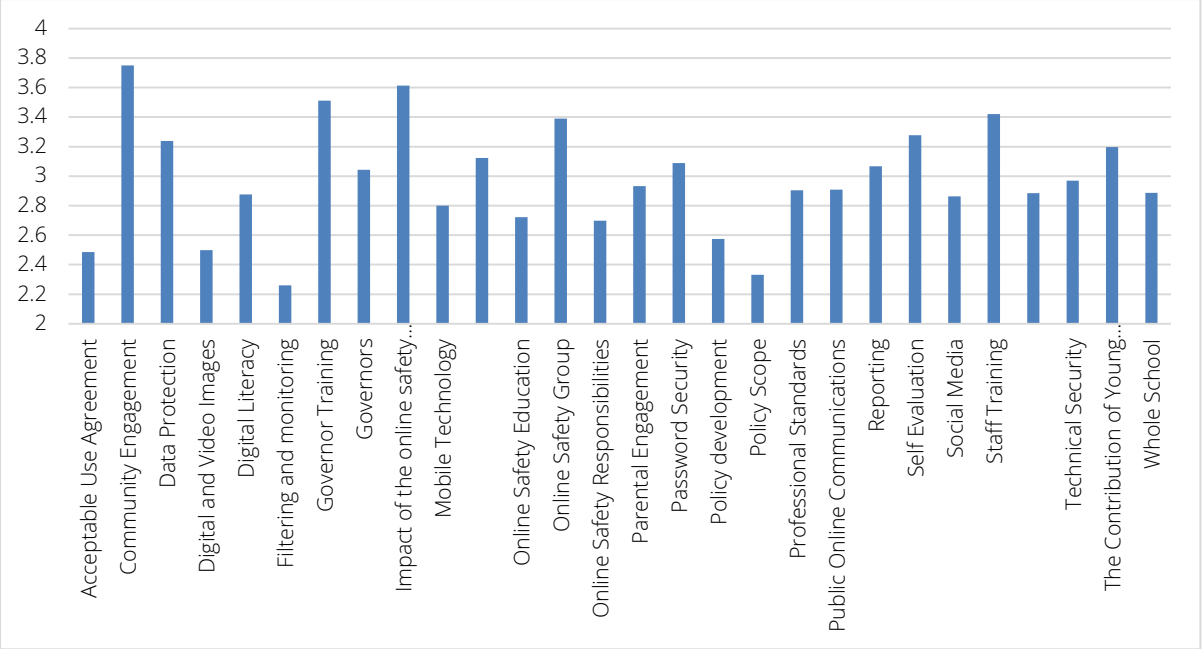
5. Analysis of the Dataset – State of the Nation 2016

Following on from activity analysis, this top level review of the 360 database explores what we refer to as the "State of the Nation". This applies basic descriptive statistics to the database to get an overall picture of the data. This therefore allows us to understand where online safety policy and practice is, in general, what are the areas of strength and weakness? However, we should present our standard caveat about this analysis – we can only analyse the data returned by schools who have chosen to engage with the tool therefore, arguably, this will represent those who are more committed to online safety than those who do not. We would suggest that the statistics presented here are better than the overall national provision.

However, as will be discussed below, we can see that the State of the Nation "shape" differs over time which gives us confidence that the dataset shows a true assessment of schools' practice and policy among 360 degree safe users.

As discussed in section 2, each aspect can be rated by the self-reviewing establishments on a progressive maturity scale from 5 (lowest rating) and 1 (highest). Therefore, taking a mean score of every establishment gives us an indication of strength and weakness in online safety policy and practice across all schools in the database. Figure 5-1 illustrates overall averages across aspects:

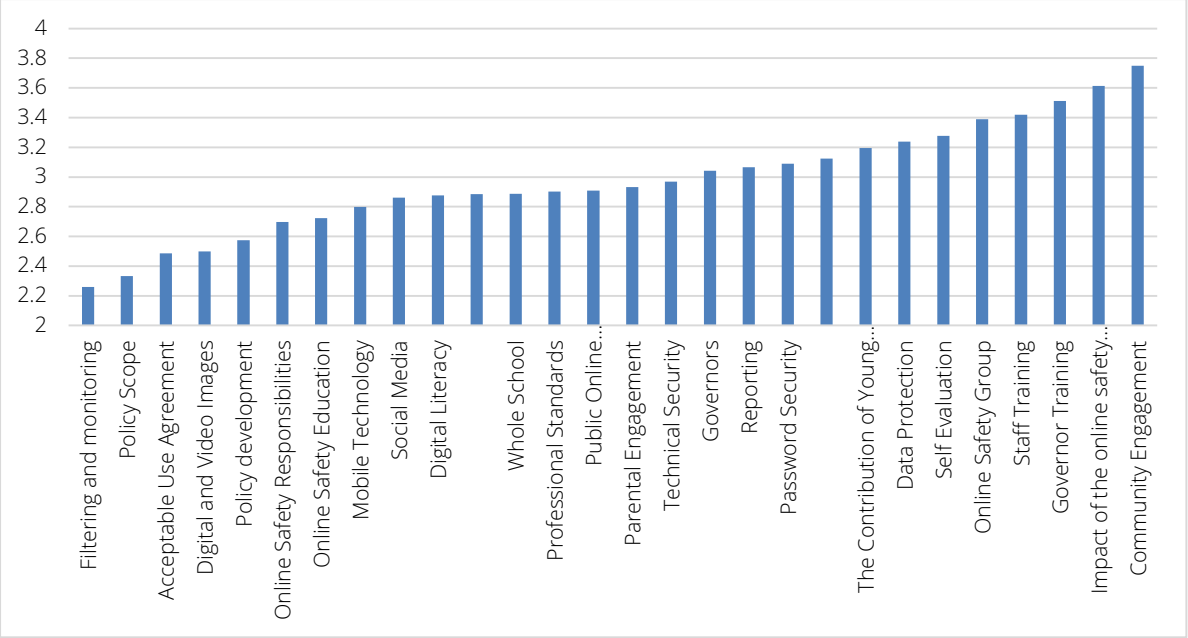
Figure 0-1 - Average rating per aspect



From this initial analysis, we can see a range of average ratings across the different aspects of online safety policy and practice. Bearing in mind that the smaller the column, the better the average rating, we can see, as is usual with the analysis, that there is strength in areas such as Connectivity and Filtering, Acceptable Usage Policy, and Policy Scope, all of which are below a mean of 2.5, with filtering being particularly strong. In general the strongest areas are those that relate to policy or technical infrastructure. However, again as with analysis in other years, there is far less strength in those areas that require a longer investment in time or regular monitoring. So aspects such as Governor and Staff Training, Community Engagement and the Impact of Online Safety Policy, have values of over 3.5. Therefore with all of these important aspects, particularly related to the training of both staff and governors (those who are keys to holding schools to account) are showing that, in general, there is only either planning or no activity in place.

Figure 5-2 orders the aspects from strongest to weakest and more clearly illustrates these points.

Figure 0-2 - Average rating per aspect, ranked



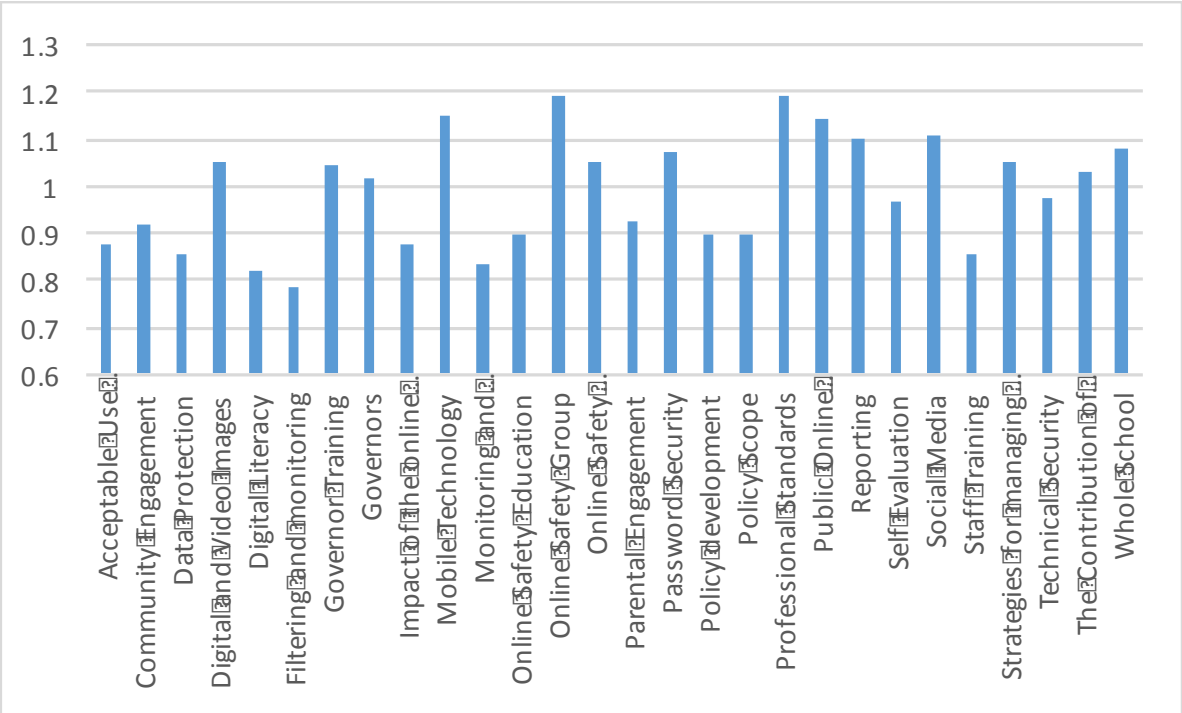
More explicitly, the strongest aspects are:

- Filtering and monitoring (2.26)
- Policy Scope (2.332)
- Acceptable Use Agreement (2.486)
- Digital and Video Images (2.499)
- Policy development (2.575)

And the weakest are:

- Community Engagement (3.749)
- Impact of the E-Safety Policy and Practice (3.614)
- Governor Training (3.512)
- Staff Training (3.42)
- Online Safety Group (3.39)

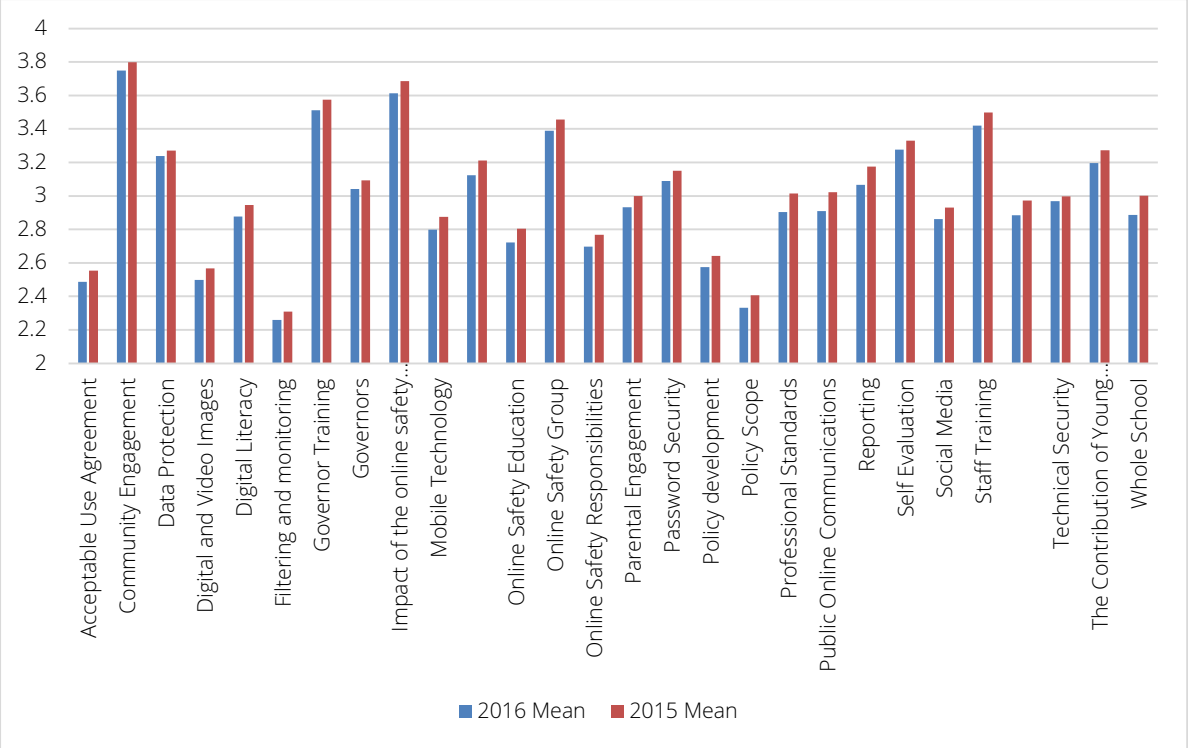
If we take another statistical measure, we can look at the range of responses per aspect. Standard deviation defines how spread out a range of results are an in this case allows us to explore how diverse each aspect is in terms of school response, the higher the value, the greater the variability of response.



Again the picture with standard deviations is consistent with previous analyses. Some of the more alarming aspects are those where performance based upon aspect mean is clearly weak – such as staff training and community engagement – and also have a narrow standard deviation. This means that performance across the entire data set is weak. Equally, a strong aspect such as Filtering and Monitoring has a narrow standard deviation, meaning that it is consistently strong across establishments. An area such as Governor Training, a very important aspect given the challenge they can provide senior leaders is schools, shows greater variability in responses, so there will be some schools that have better performance than others. Equally a policy area such as Mobile Technology, has a very broad standard deviation, showing the variability in practice across schools.

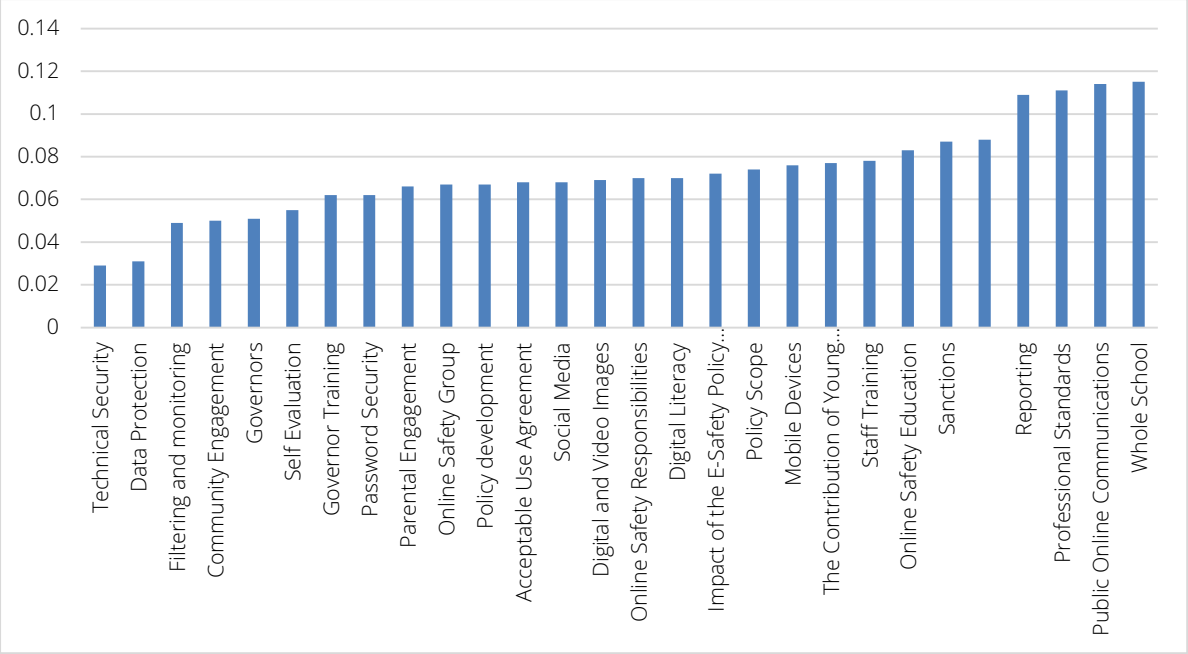
In figure 5-4, we show a comparison of 2015 means with those from 2016. It shows that, once again, there has been overall improvement across all aspects. While improvements are, on the whole, small, all 360 degree safe schools are improving globally.

Figure 0-3 – Comparison of 2015 and 2016 means



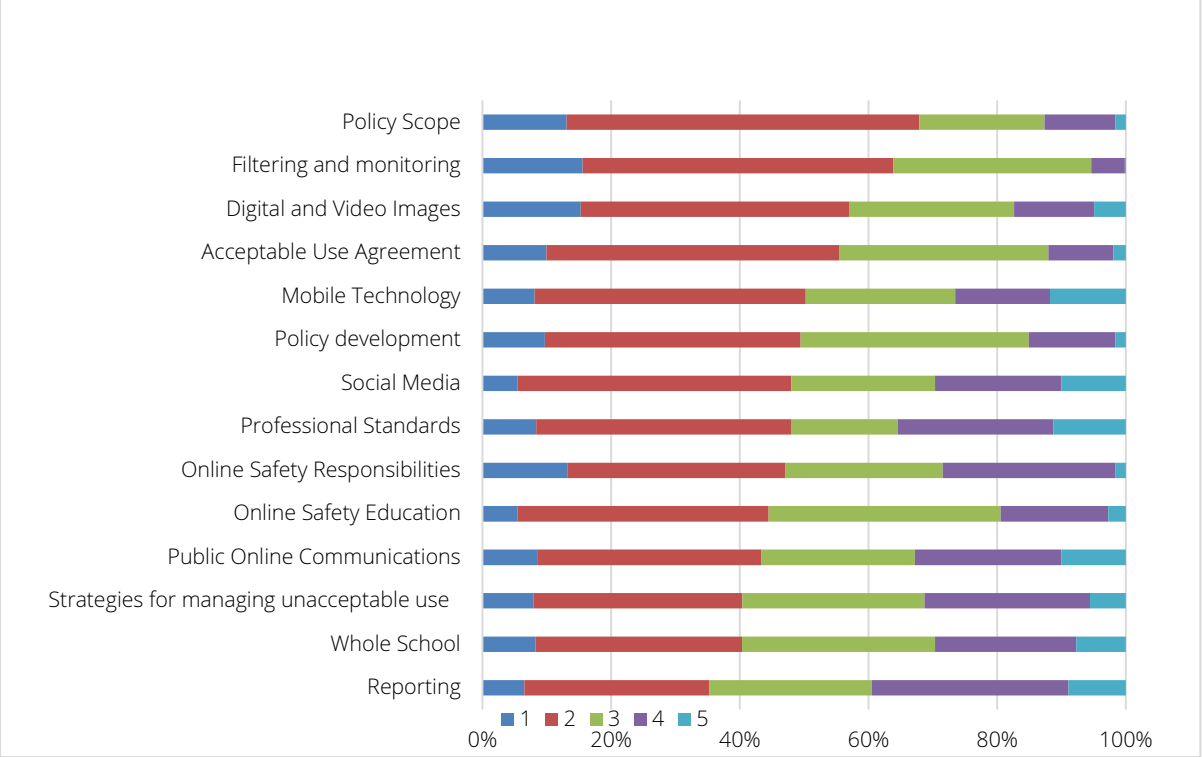
However, if we order these changes based upon the difference between the 2015 and 2016 means (figure 5-5), we can see in some cases the improvements are very small indeed, particularly those around data protection issues and also community engagement.

Figure 0-4 - Difference between 2015 and 2016 means



A final analysis of the overall dataset, which provides a different perspective on the distribution of levels in each aspect, breaks down the proportion of each aspect where establishments have evaluated themselves per level. This is clearly illustrated in figures 5-6 and 5-7. Figure 5-6 shows the stronger aspects, ordered by the number of establishments that have rated themselves either 1 or 2.

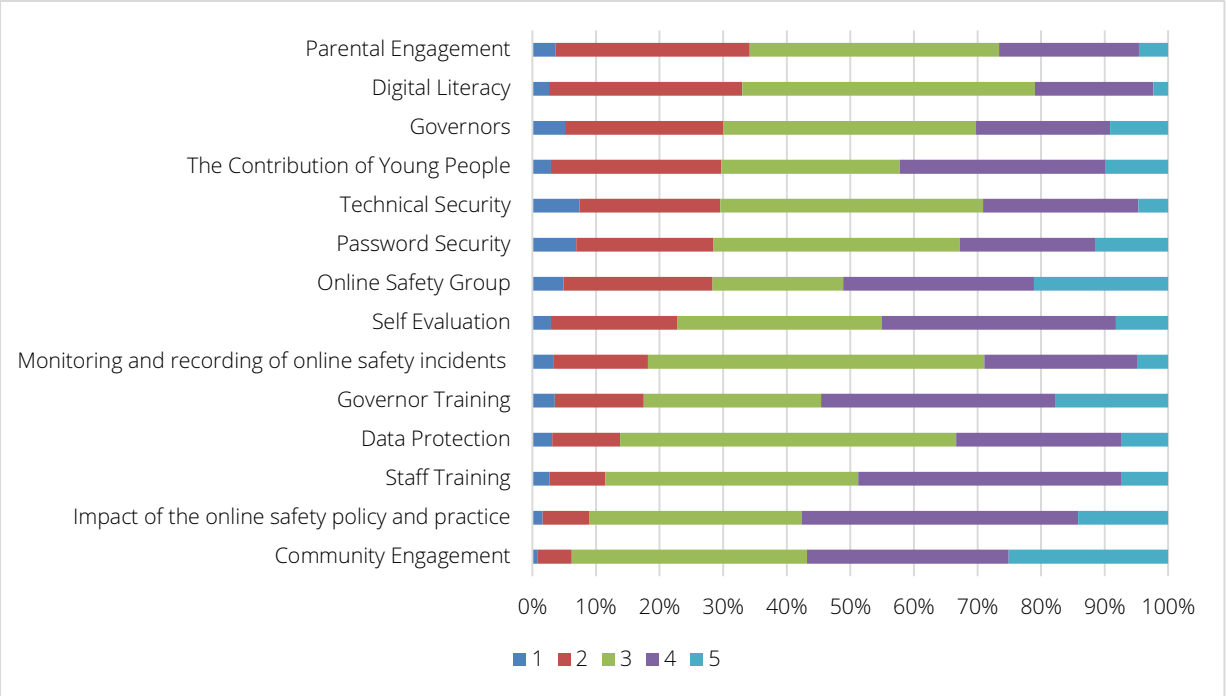
Figure 0-5 - Distribution of ratings per aspect – stronger aspects



This distribution analysis provides us with a different perspective which confirms some of the findings from the descriptive statistics, but also draws out other interesting developments that aren't immediately apparent from initial analysis. For example, it does confirm that the stronger aspects generally centre on policy and infrastructure issues – there are positive conclusions to be drawn from this figure:

- Almost 65% of schools have excellent or good connectivity and filtering in place
- Almost 55%% have a detailed and effective Acceptable Usage Agreement in place
- Only 15% of schools have nothing in practice around policy development
- Almost 70% of schools have strong online safety policies in place

Figure 0-6 – Distribution of ratings per aspect - weaker aspects



However, distributions from figure 5-7 confirm the weaknesses from the earlier analysis

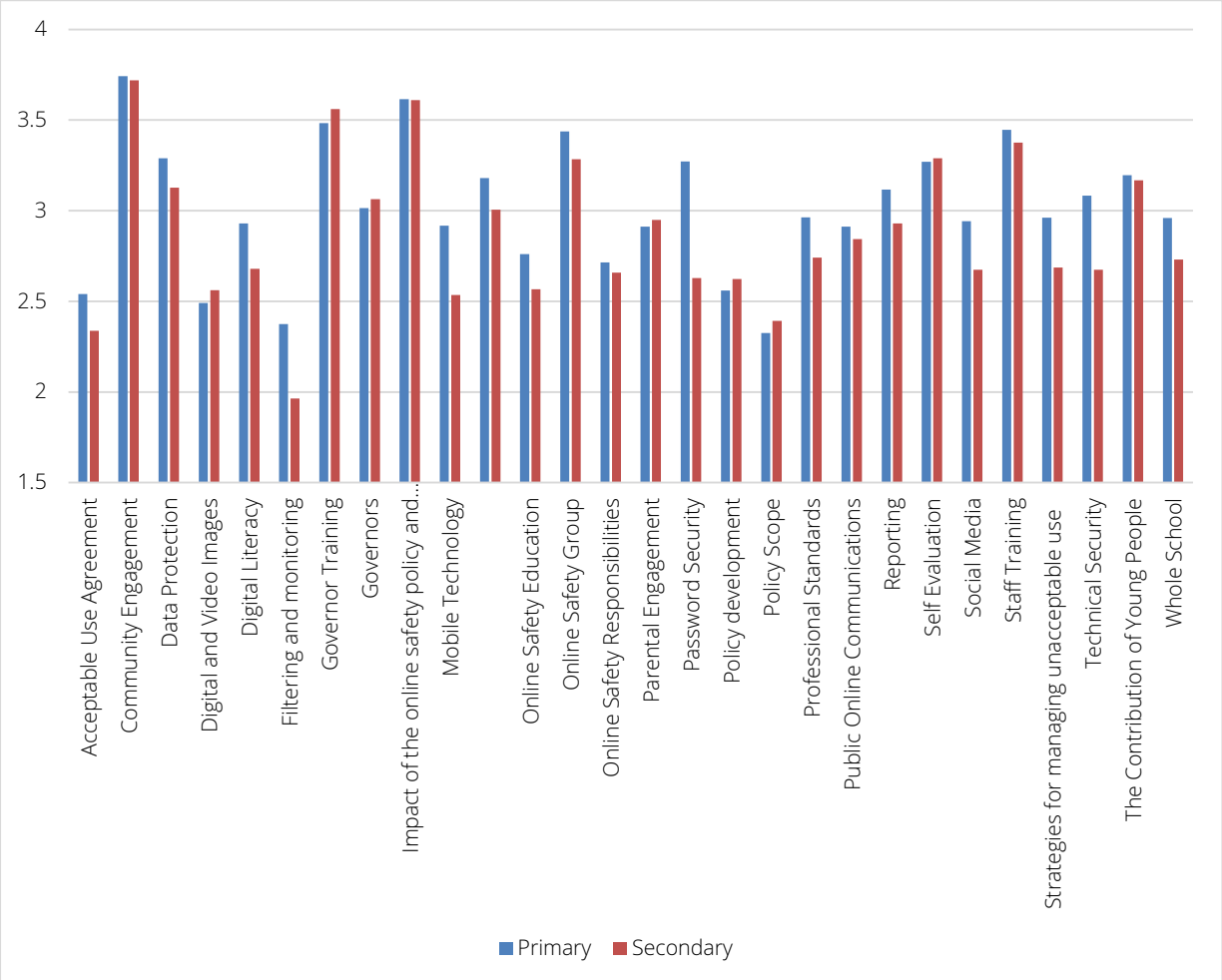
- Almost 60% of schools have no engagement with the community on online safety issues
- 55% have carried out no governor training around online safety issues
- Almost 50% have no staff training to date around online safety
- Almost 35% have no data protection policy in place, even though they are legally responsible for the secure storage of sensitive personal data about children and young people
- Over 50% of schools have no means to evaluate the impact of their online safety strategy.

6. Comparing Primary and Secondary Establishments

As a progression of the analysis as a whole, the following section considers differences between primary and secondary schools who are using the tool. In previous analyses there has been some variability in the gap between the two phases of school. In some years there has been a clear gap between the weaker primary schools and stronger secondaries. However, in general, there is greater weakness in primary schools than secondary establishments. While in some areas, such as those that require technical support, this might be expected, there are also other areas where such resourcing issues are less demanding. Throughout this section we will focus on the areas of greatest difference between the two types of establishment.

Looking at the 2016 data set, we can certainly see some difference between the two phases of school:

Figure 0-1 - Primary/secondary comparison 2015



Again, while the dataset for each phase exhibits the "shape" of data we have come to expect from this analysis, we can also see that the difference between primary and secondary practices is variable between aspects.

Table 0-1 - Primary and Secondary strongest aspects

Primary Strongest	Secondary Strongest
Policy Scope (2.396) Filtering and monitoring (2.429) Digital and Video Images (2.563) Acceptable Use Agreement (2.615) Policy development (2.626)	Filtering and monitoring (2.018) Acceptable Use Agreement (2.378) Policy Scope (2.447) Mobile Devices (2.572) Digital and Video Images (2.607)

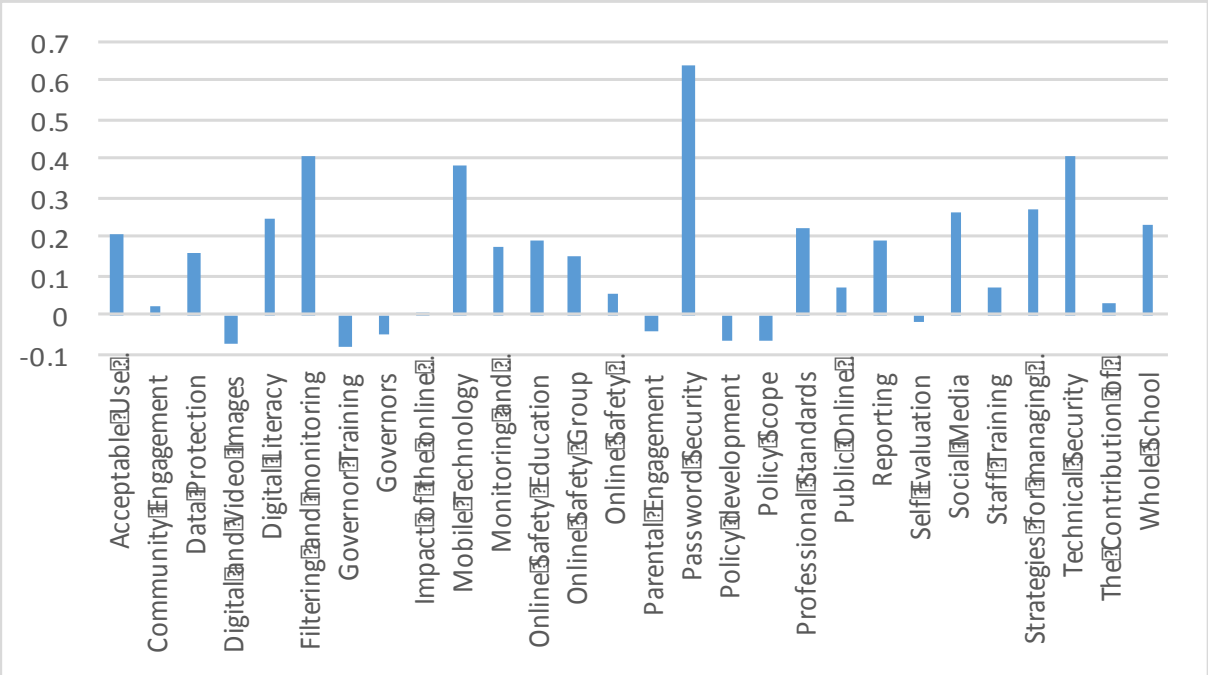
Table 0-2 - Primary and secondary school weakest aspects

Primary Weakest	Secondary Weakest
Community Engagement (3.801) Impact of the E-Safety Policy and Practice (3.695) Governor Training (3.545) Staff Training (3.524) E-Safety Group (3.512)	Community Engagement (3.749) Impact of the E-Safety Policy and Practice (3.663) Governor Training (3.604) Staff Training (3.445) E-Safety Group (3.348)

For the weakest aspects, we can see they "rank" similarly but with Secondary schools performing slightly higher than Primary schools

The differences are more clearly illustrated in figure 6-2, where a value below zero indicated between values coming from the primary data set are stronger and above the line showing strength in secondary schools. This also highlight where the differences are the largest:

Figure 0-2 - Difference in average ratings between primary and secondary schools



In figure 6-2 we can see that, as previously mentioned, areas of technical security (Technical Security, Filtering and Monitoring, Password Security) all have greater strength in secondary schools. Most significantly there is a considerable difference in practice around password security. While this might, to some extent, be expected given the generally lesser technical resource available in primary schools, equally primary schools still have to manage sensitive data in a secure manner and manage device access. One might argue that this is even more important in primary schools, given the age of the pupils in their care. Mobile technology also continues to be an area of significant difference which, again, at face value might seem reasonable given the age of pupils but we can see from research such as OFCOM's Media Literacy tracker[4] that younger and younger children own their own mobile devices.

[4] https://www.ofcom.org.uk/research-and-data/media-literacy-research/children/children-parents-nov16

Figure 0-3 - Differences in distribution of aspect levels

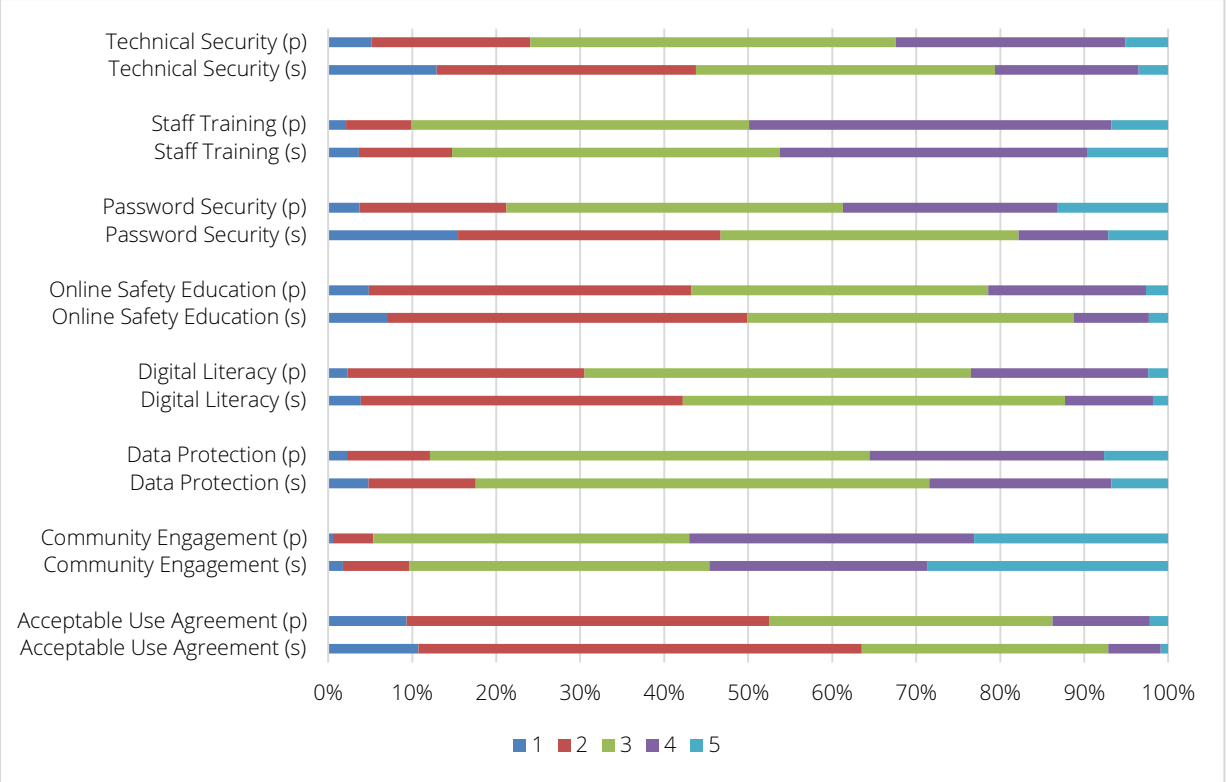


Figure 6-3 shows the percentage breakdown per aspect between primary and secondary schools comparing those where the weaker levels (those returning a 4 or 5) are most significantly different. This highlights establishments that have no practice or are only in the planning stages. From this data we can conclude that:

- 50% of primary schools have no staff training in place
- A third of primary schools have no strategy around technical security
- Over a third (35%) of primary schools do not meet statutory data protection requirements
- Almost 40% of primary schools have no policy around passwords and only basic access control mechanisms on their devices
- Almost 60% of primary schools, and 55% of secondary schools, have no community engagement practice in place.
- Almost 25% of primary schools have no education around digital literacies in place

7. Issues Arising

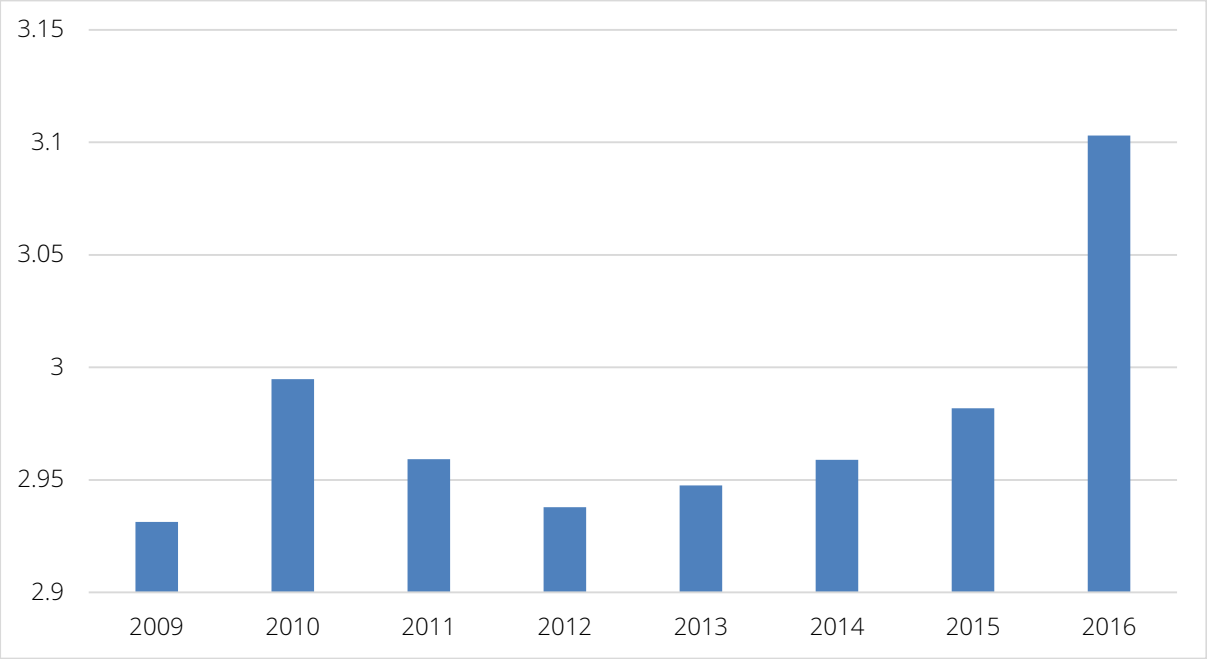
This report has provided a top level analysis of the 360 degree safe database as of November 2016 in order to develop an understanding of the health of online safety policy and practice in English schools. This is the sixth analysis of the data since its inception in

2009 and there are a number of issues that we are used to seeing in this analysis such as strength in policy and technical infrastructure, weakness in training and community engagement, and stronger performance in secondary schools than primary schools. However, it is worthwhile to explore a number of this year's findings in more detail, for different reasons.

Starting Point

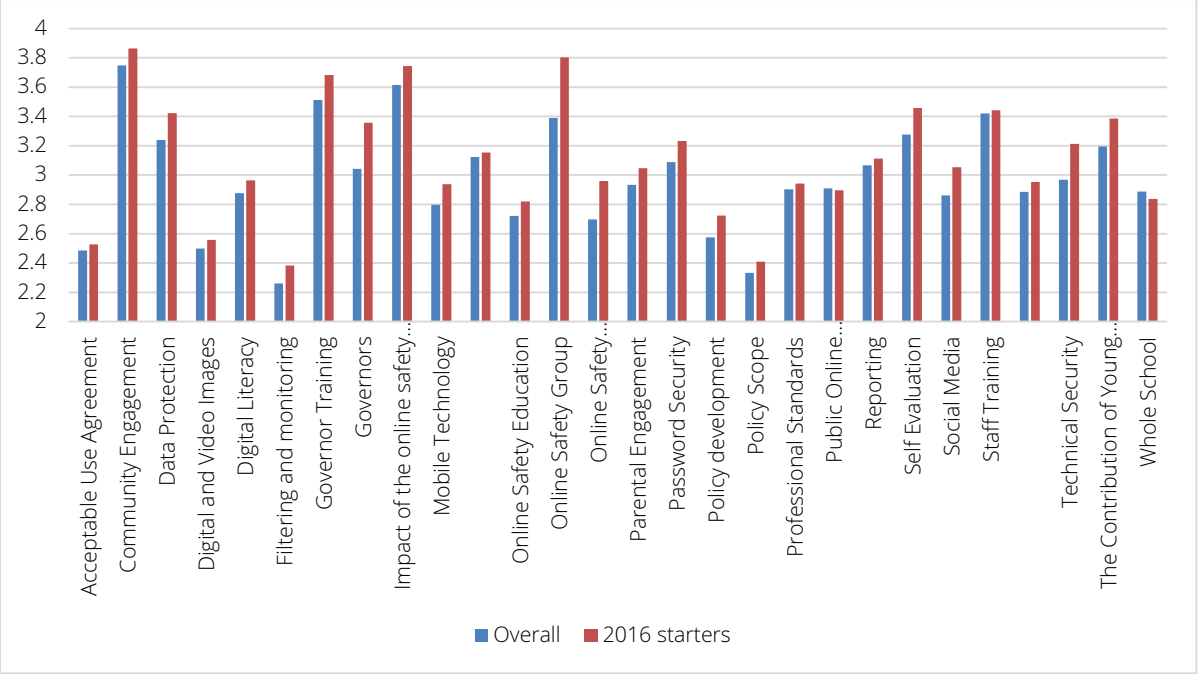
Those embarking on the use of self-review now are starting from a lower baseline that those before. In figure 7-1 we have a graph that shows the cumulative average score (i.e. the average over all 28 aspects) for establishments registering in a given year.

Figure 0-1 - Overall average starting value per year



What this graph clearly shows is there is an increasing in this average since 2012 (with a marked increase this year) – meaning the starting point for these new establishments is getting weaker that those who were earlier adopters of the tool. Certainly when we compare the profiles of 2016 adopters with the overall averages across aspects, we can once again see that those starting now are weaker:

Figure 0-2 - Comparing average ratings with 2016 adopters



This is certainly an emerging issue, and one we will return to with next year's analysis.

Issues around training

While this is a recurring issue, this is something that should be reiterated. The foundation of educational practice around online safety in a school is the knowledge of the staff at the school. If the staff are not knowledgeable about online safety issues they are not going be able provide effective education for the young people in their care, to inform policy and strategy effectively, or to communicate with the wider school community around digital matters.

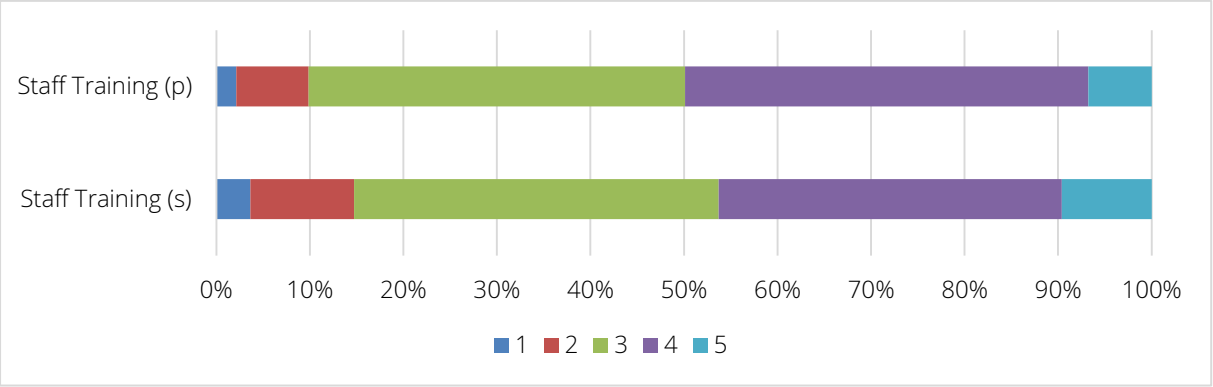
Yet staff training has always, over the 6 years of analysis of this data, been one of the weakest performing aspects. As reviewed in table 7-1, overall, with a mean of 3.43, we can say that on average schools are below the expected threshold for effective staff training. The standard deviations also show that this is a problem across the whole dataset – there are few schools that have inspirational practice around staff training.

Table 0-1 - Overall statistics for staff training

	Mean	Standard Deviation
Overall	3.42	0.855036267
Primary schools	3.446	0.815948884
Secondary schools	3.375	0.931793682

Figure 7-3 shows an even more worrying illustration from the data:

Figure 0-3 - Staff training in primary and secondary schools - distribution at each level



In 50% of primary schools and almost 50% of secondary schools, staff training is either non-existent or "in planning". Therefore, we can conclude that the school with level 4 or 5 in staff training have not received any professional development around online safety issue:

> **Level 5**
>
> *There is no planned online safety training programme for staff. Child Protection / Safeguarding training does not include online safety.*
>
> **Level 4**
>
> *A planned online safety training programme is being developed, which aligns with Child Protection and Safeguarding training.*

However, possibly more concerning is the data around governor training. Boards of governors are, in the majority of schools, the main challenge to the senior management team. Indeed, the recent Department for Education safeguarding statutory document

(Keeping Children Safe in Education, paragraphs 67-69)[5] stated that governors are responsible for "appropriate filtering and monitoring" in schools and also for ensuring effectively online safety education.

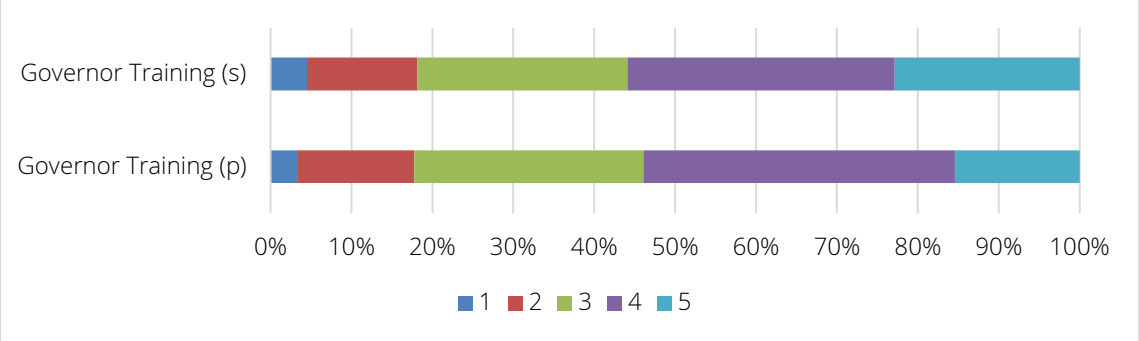
However, drawing from the data on Governor Training in the database, shown in table 7-2, we can see that the means for this are even weaker than for staff training.

Table 0-2 – Overall statistics for governor training

	Mean	Standard Deviation
Overall	3.512	1.046365591
Primary schools	3.483	1.022377477
Secondary schools	3.561	1.117399709

Coupled with figure 7-4, and reflecting on the DfE guidance, we would have to argue that while governors may be expected to hold schools to account on online safety matters, they will not have the requisite knowledge to provide effective challenge.

Figure 0-4 - Governor training in primary and secondary schools - distribution at each level



Over 50% of both primary and secondary schools have reported there is no governor training around online safety. If we consider the level 5 and 4 definitions within the 360 degree safe tool, it is clear that over half of all schools within the database have had no training for governors.

[5] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Level 5

There is no opportunity for Governors to receive online safety education.

Level 4

Opportunities for Governor online safety education are being explored.

Clearly this is a cause for concern and something that needs raising at a national level. If we are to be confident in online safety policy and practice in schools we need to know that they have staff that are knowledgeable and up to date on these issues and have effective challenge from their boards. Without these the foundations of online safety policy and practice in our schools will be very weak indeed.

Data Security

Aspects around data security have, until now, not been the focus of any concerns from the data drawn from the 360 degree safe Tool – traditionally policy and technical elements within the tool have been middle to high ranking in terms of performance and while, as with all aspects, this could be better, there have been sufficient evidence to suggest that it is something in schools that is being managed:

Table 0-3 - Overall data security aspect performance

	Average	Standard Deviation
Data Protection	3.239	0.854515811
Filtering and monitoring	2.26	0.784181853
Password Security	3.089	1.074195194
Technical Security	2.969	0.974376904

However, as illustrated in table 7-4, this is one part of online safety where there is clear difference between primary and secondary settings.

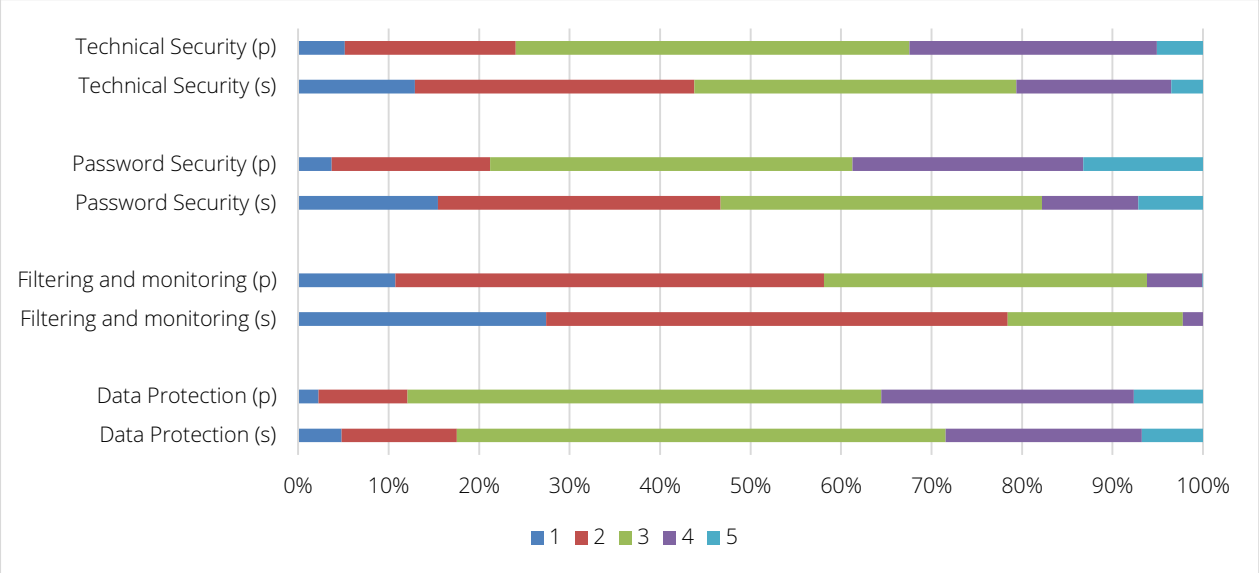
Table 0-4 - Differences between primary and secondary schools around data security.

Primary Schools	Average	Standard Deviation
Data Protection	3.289	0.830844993
Filtering and monitoring	2.374	0.758889317
Password Security	3.271	1.017732593
Technical Security	3.083	0.930805995

Secondary Schools	Average	Standard Deviation
Data Protection	3.128	0.889462624
Filtering and monitoring	1.964	0.745447516
Password Security	2.628	1.088599085
Technical Security	2.674	1.015825898

While in general secondary schools are performing well around data security aspects, this is not the case with primaries – primary schools, particularly around data protection (policy related to the safeguarding of personal data) and password security, have fairly low average ratings and this is also borne out when we look at distribution of levels:

Figure 0-5 – Data security aspects comparing primary (p) and secondary (s) schools - distribution at each level



Taking each one of these in turn, looking at the lower level descriptions in the tool, for technical security we can see than over 30% of primary schools are at level 5 or 4. While

level 4 shows that there are some access control mechanisms in place, there is nothing that forms part of an integrated strategy.

Technical security

Level 5

The school has no strategy to plan, manage or monitor the technical and physical security of its systems and devices and the safety of its users

Level 4

The school is developing its technical security strategy. Senior Leaders understand their responsibilities regarding the provision of safe and secure technologies for all users and drive strategy development. There are clear mechanisms for network access that include user identification for all users (where age appropriate). The technical and physical security of devices and network equipment has been considered and is being implemented, including the network identification and management of devices.

Almost 40% of primary schools have password security at either level 5 or 4, again showing that at best schools will have very basic password mechanisms that do not form part of a policy or strategy. Perhaps most concerning at this level is that individual logins for students do not exist – therefore making it very difficult to audit student behaviour on devices.

Password Security

Level 5

The school has no password policy or practices in place to protect the security of its systems and data.

Level 4

The school is developing a password policy and practices to protect the security of its systems and data. A system for managing passwords is in place, with responsibilities allocated. Appropriate staff use passwords for access to networks and devices and have received training. There are age appropriate password requirements for pupil / student user access.

While Filtering and Monitoring is consistently the strongest aspect within the analysis of data from the tool, it is worth mentioning that almost 10% of primary schools report that they are level 4 for this aspect. While filtering is in place at this level, it is not, to the knowledge of the school, updated or monitored. Again, given the constant change in online content and its location, this is cause for concern.

Filtering and Monitoring

Level 4

Internet access is filtered for all users, but the filtering is neither regularly monitored nor updated. Illegal content (e.g. child sexual abuse; extreme pornography or criminally racist or terrorist content) is filtered by actively employing illegal content lists (e.g. IWF CAIC list). Filtering should also include mechanisms to protect users from accessing terrorist and extremist material and prevent people being drawn into terrorism (Counter Terrorism and Securities Act 2015).

Just under 30% of secondary schools and over 35% of primary schools have Data Protection at either level 5 or 4. While 8% of primary schools have no policies at all that relate to Data Protection, even at Level 4, as illustrated below, compliance with statutory data protection obligations is not met.

Data Protection

Level 5

There are no policies ensuring compliance with legal, statutory, regulatory and contractual data requirements. The school has not yet registered with the ICO.

Level 4

The school is developing a comprehensive Data Protection Policy. The school has registered with the ICO. Parents and carers are informed about their rights and about the use of personal data through the Privacy Notice.

If we combine these aspects together to paint a picture of data security practice in schools, we can see for a small but significant minority of primary schools (in particular) there is potential for personal data to be at risk of attack or compromise.

Without effective data security, and with growing concerns around data protection and more complex ways to attack all manner of IT systems, this is something we need to raise, given what the 360 degree safe data is telling us. While a primary school might not see themselves as being the target for criminal activity we can see an increase in, for example, financial extortion through Ransomware [Trend Micro – 2016 Security Readiness Survey[6]] whereby an attacker is simply looking to prevent an organization from accessing their own data without paying to regain access over their systems. Such attackers will go after organisations that have weak security, and we have certainly seen in increase in schools being targeted for such. All schools hold sensitive data on young people and as such need to take data protection issues very seriously if they are to avoid attack or legal penalty, which might occur is a data breach occurs.

8. Conclusions

This 6th review of the 360 degree safe database presents both familiar and unfamiliar findings. On the one hand, we still see a similar "shape" to the data, with strength in policy and infrastructure aspects, and weakness in those that require longer term resource investment, such as training and community engagement. We are also seeing a small, but consistent, increase in average performance across the whole data set, which is encouraging because it shows that overall things are improving around online safety policy and practice in schools.

We have also seen that the usual weakness around training still exists, but becomes more concerning given the increasing complexities around young people's use of digital technology, and the risks that are introduced through their use. Moreover, the greater expectation of governors to be the main challengers to strategy in many schools means that it is essential they are well informed around online safety issues to be able to challenge effectively in this area.

Finally, we have growing concerns over data protection and information security, particularly in primary schools. Given the increase in extortion based attacks, the growing amount of personal data managed and obligations, it is important that schools recognise the importance of effective data security strategy and implement it effectively.

[6] http://www.trendmicro.com/vinfo/us/security/news/security-predictions/ransomware-attacks-incidents-consistent-with-security-survey-results