Understanding cyber security requirements in mainstream schools

Abstract:

This paper aims to better understand the main areas of cyber security implementation and education needed within a school setting. These have been analysed under five areas, namely: pupil cyber safety; pupil cyber security knowledge; teacher training in cyber safety; teacher training in cyber security knowledge and school system cybersecurity. Any overarching school offerings separate from these headings which may feed into cybersecurity education will also be investigated. This is to discover current cybersecurity plans in place, those ideas which are in progress and if any further recommendations fall out of investigations.

Introduction:

Technology has undergone a massive acceleration in recent years. It is only within 25 years that cyber security threats stopped becoming just the preserve of governments and started to threaten the public at large [4]. Schools contain a wealth of data on school pupils, from medical records to dates of birth and academic achievement along with payment systems for lunch and school trips. Schools are therefore as much of an attach target for hackers as any other institution.

Market predictions for future employment is heavily skewed towards computer technology [25]. The UK government in particular have stated their intention to create a 'self-sustaining pipeline of talent' within cybersecurity and having a cyber security literate population [15]. It is still the case though that both domestic and global markets are regularly reporting unmet demands for cyber security skills [1, 16].

In addition, concerns are not just about school systems and future employment but on technologies impact on the mental health and safety of young people – especially social media influences. An Organisation for Economic Co-operation and Development (OECD) report covering 48 countries and experiences of a quarter of a million teachers showed particular issues with cyber-bullying within English schools [24].

Those responsible for providing these requirements are actively seeking help in order to fulfil their obligations [26, 27, 28, 29]. Schools along with industries are facing the challenge of how to educate their current staff to provide learning for pupils in these areas of cyber security, recruit within areas of need and continue keeping their own systems secure against attack.

Research will look into these issues to understand the current situation within the UK state school system. These finding will be viewed within the wider area of UK recruitment to determine if there is anything else which could be of benefit in this area along with areas of further research.

Methodology:

Government documents and industry reports will inform much of the learnings into what is formally required of schools as well as that which is guidance for the education sector. Research into any relevant academic papers will also be completed.

Knowledge of pre-school, infant school and junior school curriculum through a parental capacity will also inform learnings as to what is offered at these key stages [26, 27, 28]. In addition, visits to a secondary school in the role of lead governor of curriculum, education and outcomes [29] will enable an overview of this stage of learning. Background to the schooling system and national curriculum framework is also known to the researcher through historically working for 2 years as a teacher, previous mentoring roles (of both pupils and teachers) as well as other previous governor roles within state schools.

The researchers background within the education sector is very useful for investigation but it should also be noted that this has the potential to bias responses and also my interpretation of documents used in research. The researcher is mindful of this, especially when using learnings from visits as a governor capacity regarding information given from teaching staff.

Background to UK school structure:

The UK the schooling system is split into fee paying (private/public schools) and non-fee paying (state) sectors. This report focusses on state schools, however, it is noted that private/public schools will be affected by similar areas, maybe even more so from systems being hacked due to the large amounts of fees charged making an attractive target for criminals.

There are 30,451 state schools within the UK [30] which gives the need to ensure policies on cybersecurity are implemented uniformly across institutions. The national curriculum is the programme of study produced by the Department for Education which ensures nationwide uniformity of standards and contents in education. The Office for Standards in Education (Ofsted) have the responsibility for inspecting and regulating services which care for children and ensuring the curriculum is being implemented appropriately. Cybersecurity promotion specifically, however, would fall under the Department for Digital Culture, Media and Sport (DCMS).

Figure 1 gives the structure of the UK schooling system from birth to 18 years. This guide shows that there is not always a simple match between the way the government splits out the key stage learnings and the school institution intake.

<table>
<tr><td>Age at 1 Sept</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td></tr>
<tr><td>School year</td><td colspan="4"></td><td>rec’n*</td><td>Yr 1</td><td>Yr 2</td><td>Yr 3</td><td>Yr 4</td><td>Yr 5</td><td>Yr 6</td><td>Yr 7</td><td>Yr 8</td><td>Yr 9</td><td>Yr 10</td><td>Yr 11</td><td>Yr 12</td><td>Yr 13</td></tr>
<tr><td>Key stage</td><td colspan="5">EYFS</td><td colspan="2">KS1</td><td colspan="4">KS2</td><td colspan="4">KS3</td><td colspan="2">KS4</td><td colspan="2">KS5</td></tr>
<tr><td rowspan="3">School type</td><td colspan="2">Nursery</td><td colspan="5">Primary School</td><td colspan="6">Secondary School with sixth form</td></tr>
<tr><td>Nursery</td><td>Preschool</td><td colspan="3">Infant school</td><td colspan="3">Junior school</td><td colspan="4">Secondary school</td><td colspan="2">Sixth form</td></tr>
<tr><td colspan="2">(Childminder)</td><td colspan="4">Lower school</td><td colspan="3">Middle school</td><td colspan="3">Upper school</td><td colspan="2">College</td></tr>
</table>

Figure 1: Summary of school types, key stages and school years for ages of pupils, *rec’n = reception

Five STEPS of cyber security:

There are numerous reports in government reports and mainstream media about cyber security in education. However, this often results in a broad topic becoming confused, as schools are expected to develop skills across many, very different, areas. These areas have been segregated into five STEPS, shown in fugure 2, as a starting point which will be analyse in turn.

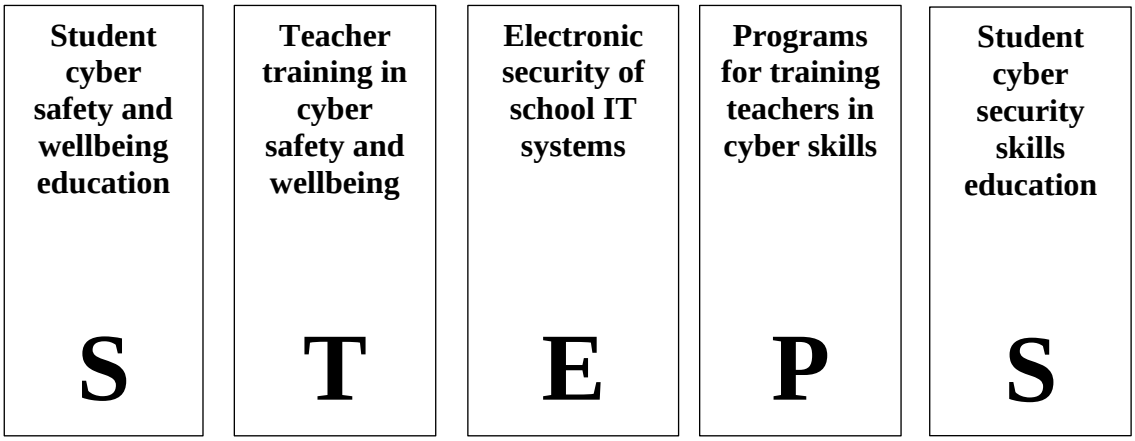

Figure 2: Five steps used for examining cyber security in schools

1.Electronic security of school IT systems:

'Whilst it was hospitals rather than schools which suffered major disruption from the WannaCry virus, schools are just as likely as any organization to face DDoS and phishing attacks.' [23].
Mark Bentley, Safeguarding and Cybersecurity, London Grid for Learning (LGfL)

Like businesses schools are at risk from being targets of hackers. A quick look within open source media gives many examples of schools being targeted, examples include:

- Clowne's Heritage High School in Derbyshire having to close early for the summer after its IT systems were attacked by a ransomware virus [37]. This restricted staff accessing the telephone systems, emails and school data.
- Sir John Colfox Academy in Dorset hit by a ransomware attack which encrypted files after a member of staff opened an email containing a virus. This caused GCSE coursework to be lost [36].

Schools have systems for electronic payments, such as Scopay [28], for lunches, trips, special days etc paid for by parents which are a prime target for cybercriminals. Also schools hold personal and sensitive personal data not only on their staff but also pupils. Addresses, dates of birth, educational information, medical data etc can be valuable to cyber criminals who could exploit this to a third party.

Attack on schools are now becoming all too common and successful [40]. The main reasons for this include:

- Lack of resources both in terms of staff and budget
- A culture of bring your own devices can be difficult to secure in the wider network
- Having policies and ensuring they are followed is tough, particularly in larger schools.

In an audit of more than 430 schools completed across the UK by the NCSC and LGfL nearly all (97%) said that losing access to network connected IT services would cause massive disruption [20]. Other research notes that one in five schools have been victims of cybercrime [38]. Even though the government has given advice on cyber essentials in schools, defined in figure 3, only 14% of schools have actually implemented and completed this scheme. This is an area which could be improved in the 86% of schools who do not have these in place to ensure stronger cyber hygiene.

Figure 3: Government advice, cyber essentials [39]

The introduction of GDPR in May 2018 led to schools being more aware of IT systems to ensure they were compliant with the new data protections laws [26, 27, 29]. However, this initial impetus from this regulation needs to be kept up if more schools are not going to fall victim to cybercrime.

2. Student cybersecurity skills education:

We are in the fourth industrial revolution. Advances in algorithms give machine learning, deep learning and artificial intelligence with more automation predicted to come [31]. With a future focus on technology the focus on these skills in education will be essential for a pipeline of talent from schools [15].

Academic papers from the UK on cybersecurity in schools seem noticeable by their absence. Within the UK this seems to be more covered by the government or outsourced to consultancy businesses. South Africa has done much research in this area [2], with the situation there being summarised as:

- no formal curriculum as yet addressing cyber security in schools
- being left to universities to teach cyber security principles which they currently do only in computing-related courses

Within South Africa it is noted only a very small percentage of the population (usually white males who disproportionately take computing courses at university) are made aware of cyber security risks and know how to take precautions. Within the UK there does seem to be similarities with this but with slightly more progress, with either schemes up and running which aim to address these issues or ideas in the pipeline. These are discussed further below.

The national curriculum: A strong national curriculum is crucial in providing pupils with the initial knowledge for more technical careers and developing broader digital skills increasingly vital for a digital economy [16]. Since 2014, computer science has been a statutory subject for 5-14 years in English schools [34] which provides a foundation for computational thinking.

Children have the option to follow this into computing qualification, such as GCSE [8] and A level [9]. However, these subjects still lag significantly behind other STEM subjects, clearly demonstrated by the graph below [35]. It has been noted that even within computing courses there is insufficient exposure to cybersecurity concepts [5]. Figures from the government also show less than a third of students studying STEM-related A Levels go on to gain a STEM degree.

This graph also shows the extremely low participation of females in CGSE computing with only 20% of the 2017 GCSE exam entrants - dropping to 9% at A Level [14]. ICT GCSE has also been phased out in 2018, leaving the more technical computer science GCSE as the only option. The Royal Society anticipates a further drop in GCSE uptake as a result of this change [14].

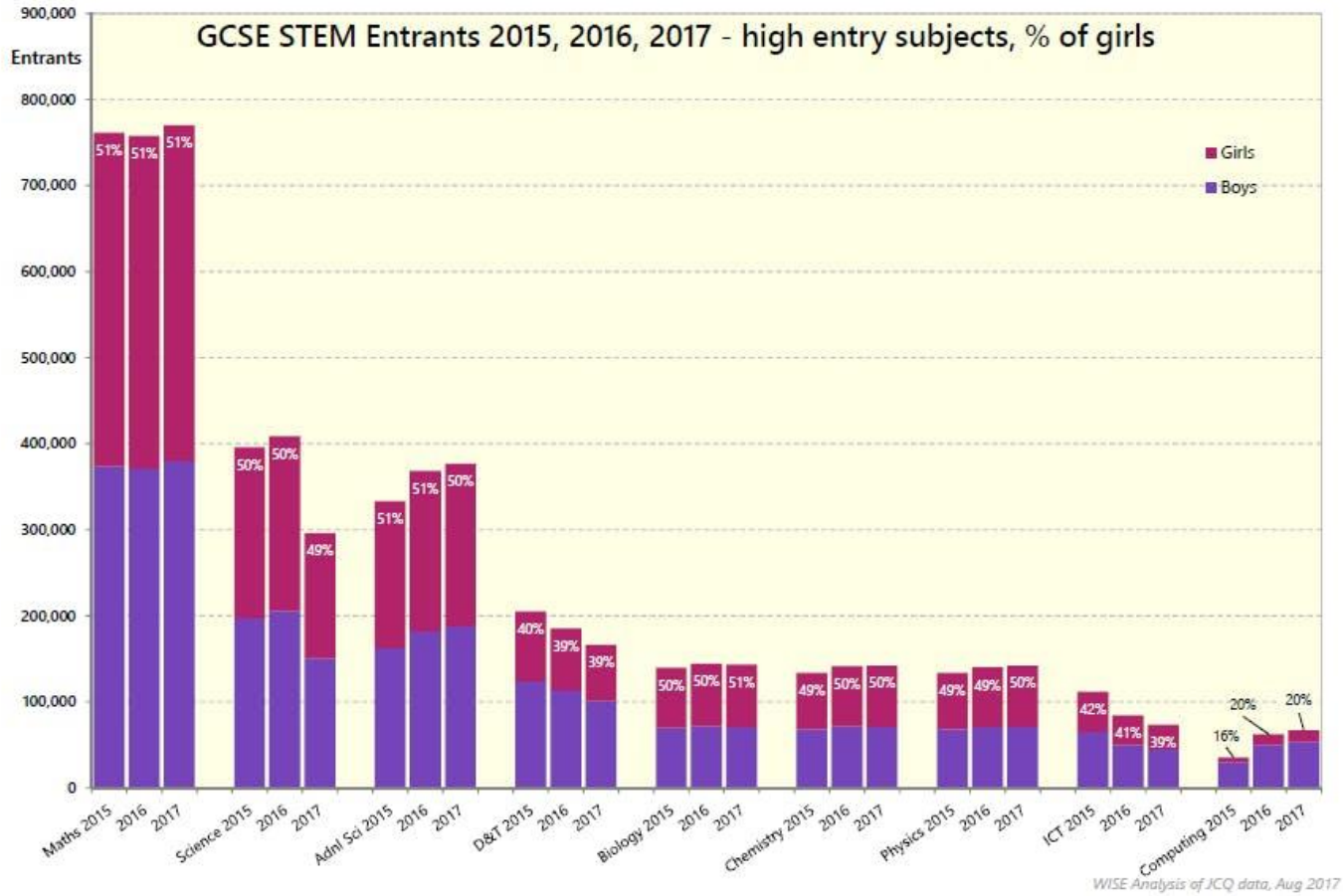

Figure 3: Computer science GCSE entrants [35]

It is not only in the computer curriculum, however, some advocate for new teaching methods should be embedded across the curricula. To develop an effective approach to cybersecurity education it is suggested that personalised, real world lesson scenarios should be added across other subjects. These would aim to capture children's interest and enhance their engagement, plus allowing them to understand day-to-day scenarios in cybersecurity [22].

Cyber Schools Hub: The NCSC has set up a Cyber Schools Hubs programme which is a pilot within 2 schools (one in Cheltenham the other in Gloucester) which aims to find ways cybersecurity education resources can be used. Their aim is to providing a potential blueprint for a schemes which could be rolled out on a national scale providing a focus for cybersecurity resources and facilitate industry engagement. The government is currently exploring how these Hubs can be expanded across England [16] to encourage a diverse range of students to take up computer science.

Cyber discovery: The governments has invested £20m in the Cyber Discovery program. This is aimed at 14-18 year olds to get them interested and inspired by real world cybersecurity experiences. Over 2 years since its launch in 2017, 23,000 students have registered on this programme [6].

CyberFirst Girls: This is another government scheme using extra-curricular activities to address cybersecurity skills shortage. With females under-represented in most STEM subjects at every stage of the skills pipeline [14] it aims to rebalance the gender variance by targeting girls studying computer science. In 2018, 4,500 girls from 400 schools participated in the CyberFirst Girls program [6].

Cyber Crime Prevent Strategy (Home Office): Prevent is aims to stop individuals from being drawn into terrorism and ensure they are given appropriate advice and support. The UK Serious and Organised Crime Strategy [33] aims to divert individuals at risk from breaking the law in cyber space into more meaningful activities. Limited evidence shows those at risk of cybercrime lack understanding of legal and ethical issues related to their actions. With the advanced skills some Prevent target audiences possess being in high demand, it is an opportunity for focus into positive cyber actions and employment.

Autist Spectrum Disorder (ASD) focussed schemes: Many of the participants providing evidence into a government survey pointed to the strengths brought to the field by 'neuro-divergent' individuals. It was noted people with ASD possessed 'a real talent for logic' [14], analytical thinking, focus and attention to detail. In the UK there are around 700,000 people on the autistic spectrum with only 16% of adults with autism in full time education and only 32% in any paid work [6]. There are currently schemes available for these pupils with ASD who have been found to have high level cyber skills in order to get this 'special interest' working for the cyber security industry [29].

Other Schemes: There are other schemes led by industry working with schools to assist in reducing the cybersecurity skills gap - such as STEM Ambassadors outreach [16]. The cyber security challenge UK take disadvantaged people or those with a troubled childhood and teaches them ethical hacking with a similar scheme run by Hacker House [14]. The raspberry Pi Foundation works with children to try and capture imagination early in primary schools, using Rasberry Pi's to run competitions and foster interest [32].

In terms of the national curriculum, the situation is quite similar to that found within South Africa (excluding the specialist Hub schools) with cybersecurity knowledge only found in the Computing curriculum. However, outside of the classroom in extra-curriculum offering there is very exciting opportunities available for children – if they, their teachers or parents know how to access them, however.

Globally the UK seem to be doing well in promoting and pushing STEM and cybersecurity education, as noted in the following quote.

'We were the first country in the G20 to put coding on the curriculum…We've overseen a major shift towards STEM subjects in our education system over the last six years, and since 2014 Maths has been the most popular A-level subject in English schools…We're building cyber security into our education systems' Philip Hammond in his Chancellors Speech on opening the National Cyber Security Centre (NCSC) [19]

3. Programs for training teachers in cyber skills:

High quality teaching is critical to achieving an increase in the number of pupils in schools who study towards computer science qualifications, particularly amongst girls and in disadvantaged areas. The Department for Education are making investment (£84m announced in 2017) to improve the expertise of computer science teachers [14]. The ideas of these programs are noted in figure 4 but the overarching aim is to ensure pupils are taught digital skills needed for future employment and teachers are empowered to deliver excellent lessons.

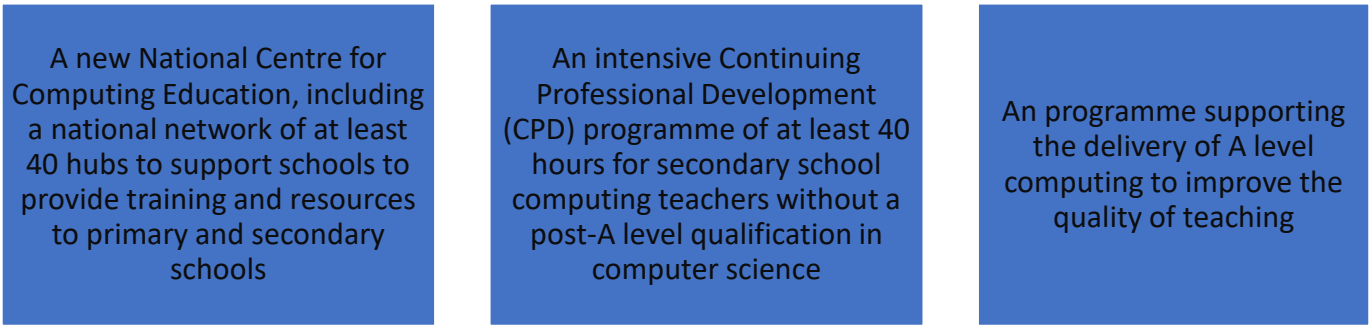

Figure 4: Department for Education programme to improve teaching of computing [16]

There is concerns over this programme, however, with teachers being expected to deliver lessons in computer science which they have not needed to learn themselves in ten years [6] – their specialism previously being ICT. A secondary school teacher notes '*ICT is like teaching someone to drive a car; computer science is teaching how the car works. I've always loved my job, but the government has asked an*

entire group of teachers to retrain to do something that they've had no prior warning of and didn't go into teaching to deliver.' [6]

The 2017 Industrial Strategy acknowledges the fact that some teachers find it challenging to deliver the computer science curriculum introduced in 2014. The quality of teaching due to this has been shown to have had an impact on the numbers of students taking computer science [14]. There is also concern lower down in schools, with the new computer science curriculum requiring coding being taught from age five. If primary teachers do not feel confident in doing this or enjoy the task asked of them then this could have a negative effect on the first association a lot of children will have with coding [26, 27].

In addition to the above noted issues computer science is also notorious in schools for being a hard role to fill when there is a staff vacancy [29]. It is not only tough to hire but also retaining highly qualified teachers given the competitive salary options available in business [14].

An idea from the NCSS is: *'supporting the accreditation of teacher professional development in cyber security. This work will help teachers, and others supporting learning, to understand cyber security education and provide a method of externally accrediting such individuals;'* [5]. However, I have not found evidence that this has been implemented to date (February 2020).

4. Cyber safety (and wellbeing) education of the pupils:

The need to be safe and secure online in order to ensure mental wellbeing is not just an area which affects pupils within schools but relevant to any organisation. However school pupils are particularly exposed to specific risks of online safety, including:

- Exposure to sexually explicit, racist, violent and extremist content
- Inappropriate contact from those who may want to abuse, exploit or bully them
- Students themselves taking part in harmful online behaviour

Guidance from the Department for Education requires school governors and managers to put into place '*an effective approach to online safety'* to *'protect and educate the whole school …in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate'* [21]

It is noted that this language is very high level and what an effective approach looks like can be quite subjective - the mechanisms to identify issues as well as a ladder of escalation could fall anywhere from extremely adequate to inadequate in answering this remit. The 'relationships education guidance' sets out what pupils should know by the end of primary and secondary school, noted in figures 5 and 6 [41].

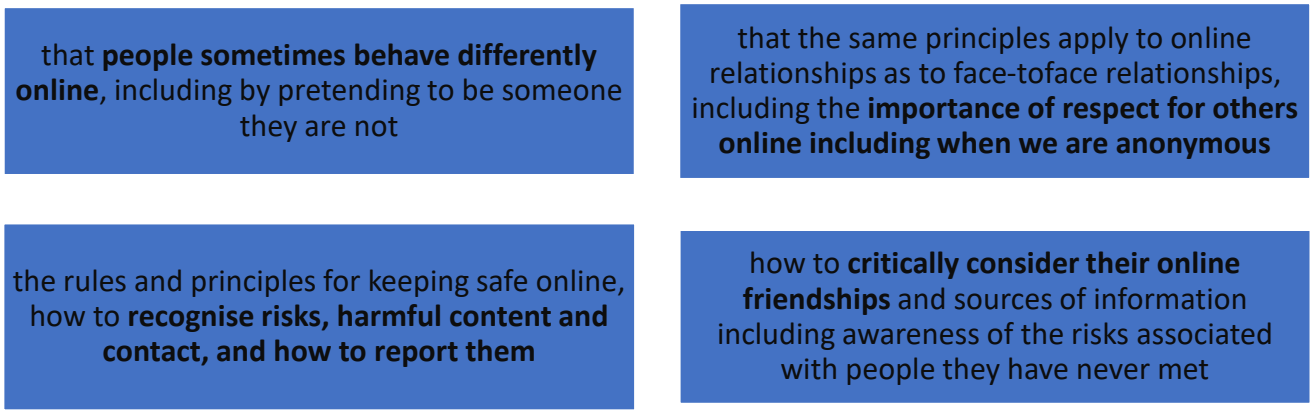

Figure 5: What pupils should know under the relationship education guidance for primary schools [41]

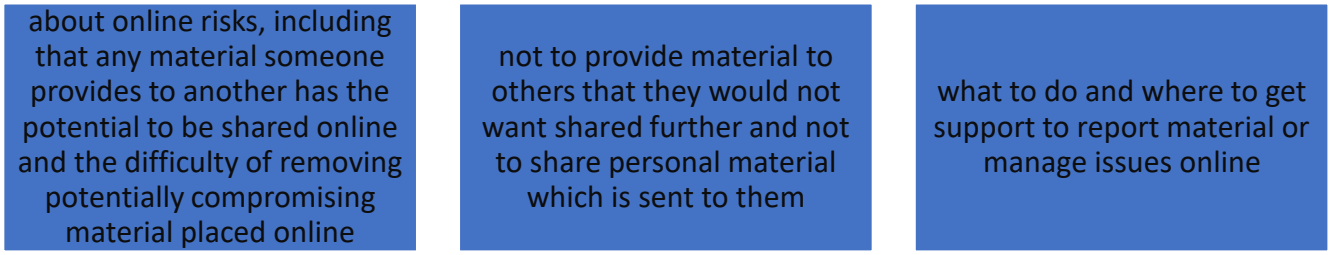

Figure 6: What pupils should know under the relationship education guidance for secondary schools [41]

During a visit to Chertsey High School I sat in on a 25 minute assembly on internet safety [29]. This was delivered by the designated safeguarding lead of the school to an extremely high standard to year 9 pupils. The contents being hard hitting dealing numerous disturbing subjects including sharing inappropriate content online and how adults can pose as children online to entice children to meet them offline. Children were informed of the feedback routes available to them and who to contact in various situations. This was not the first of these talks and cyber safety has been built up throughout the school from year 7 so the pupils were not just confronted with this information as a one off.

This example of best practice within a secondary school setting has also been observed in primary schools at an appropriate level according to age [27, 28]. The practice of having both designated days on cyber safety with special speakers coming in (from Childline for example) as well as routine backup of this on a more frequent basis (for example when online homework is set) seems a very good benchmark to aim for. Asking my own children at primary school about cyber safety teaching they seem very knowledgeable and informed over the areas they are expected to be at within their year groups.

The Chancellor speech on opening the NCSC noted: *'We're also making sure that every young person learns the cyber life-skills they need to use the internet safely, confidently and successfully.'* [19].

I see this happening in the schools I have close contact with and am confident that this is possible within these settings. What concerns me is the variation in what schools maybe offering in this area. With guidance being very subjective and also schools which maybe not as strong in teaching subjects also falling down in this area – even more concerning given these usually correlate with disadvantaged areas which maybe more in need for this education.

5.Cyber safety (and wellbeing) training of teachers:

As noted above, children need to be provided with the knowledge in order to behave responsibly and securely in a digital world. In order to achieve this end point, various frameworks have been provided by government for those who are required to teach online safety. This is particularly relevant for teaching in computer science and Personal and Social Health Education (PSHE). It is noted that PSHE is usually taught by a class form tutor in secondary schools (who looks after the pastoral care of a class in their care) or a childs regular teacher in primary schools. Both of these are non-safeguarding specialists who need to add this to their knowledge bank in addition to their teaching specialism.

There is detailed information on what is required to be taught by teachers in frameworks to support and broaden the provision of online safety and education. Two specifically I have found to be particularly useful being: Teaching online safety in schools [17]; and Education for a connected world [18].

An excerpt from teaching online safety in schools is shown in figure 7. It is noted as with Education for a connected world that this is useful in that is covers in detail what is required, but it is left to the education provider to put this into a structured learning frame to be delivered as a lesson. Some power point lesson plans were found online in this area but on closer inspection these just comprised on a copy paste of a dense case study onto one slide or similar format which is not much better than the guidance given for a busy teacher trying to get an online safety lesson together.

Potential harm or risk	Description	Curriculum area this could be covered in
Privacy Settings	Almost all devices, websites, apps and other online services come with privacy setting that can be used to control what is shared. Teaching could include: • how to find information about privacy setting on various sites, apps, devices and platforms, • explaining that privacy settings have limitations, for example they will not prevent someone posting something inappropriate.	Relationships education core content – online relationships. "the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them." Computing curriculum (all key stages) – "understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy"

Figure 7: Excerpt from Teaching online safety in schools [17]

It is noted that all schools have a designated safeguarding lead who as noted at Chertsey High School could deliver whole school education in online safety and security. These safeguarding professionals would have taken extra courses to become lead for safeguarding and will have strong contacts with the local authority for passing on concerns raised.

General teaching staff may also be required to complete online safety teaching within PSHE lessons, however, would not have as much training in safeguarding issues. Training for general teachers is usually provided by schools on their INSET training days or via online training. The ability to turn the details in guidance into practical and 'plug and play' form for teachers would be an extremely useful development in this area – allowing teachers to impart more informed knowledge required to pupils in cyber safety.

<u>Other areas informing cyber security skills acquisition:</u>

On looking through information within the education sector further ways in which cybersecurity can be integrated into schools has been noted. The focus was on skills which are harder to measure from an exam grade but are nevertheless are essential to success beyond the classroom. These are the Gatsby Benchmarks and Functional Skills discussed below.

The 8 Gatsby Benchmarks: These represent good careers guidance which schools need to self-assess against to ensure they are meeting for all pupils aged from 12-18years [39]. The 8 areas schools are required to provide are noted in figure 8. It is evident how heavily the role of third parties feature in this framework with annual contact with higher education, employers and employees. This has strong connotations to the governments overarching cybersecurity strategy of industry and academic partners delivering the skills.

These benchmarks are not specific to cybersecurity and represent a school giving their pupils an overview of future careers. However, there is an opportunity within this framework for bringing in cybersecurity careers, especially given the focus on giving pupils the knowledge of what the careers market will look like when they are out of formal education – as noted earlier data showing heavily weighting to technical skills.

The 2016 NCSS acknowledge the issue of cybersecurity careers through a commitment to by 2021 create an *'established profession with clear* pathways' and '*effective and clear entry routes ... which are attractive to a diverse range of people'* [14]. The now chartered status of cybersecurity [15] will help teachers associate cybersecurity to future training as well as just get out to education providers that this profession actually exists. An established career and training pathways from school age would also help achieve this too.

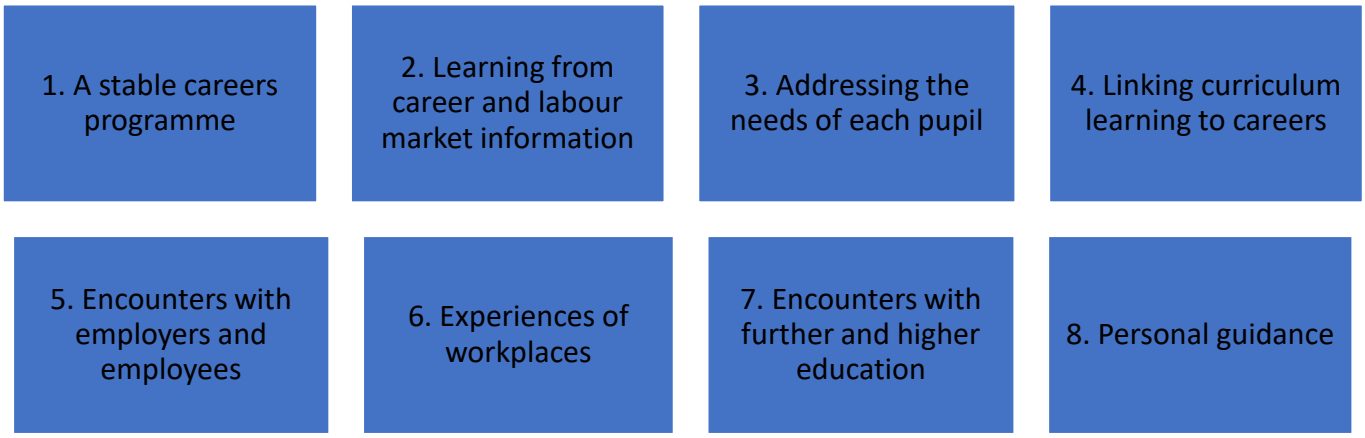

Figure 8: The 8 Gatsby Benchmarks [39]

Some weaknesses are noted within these benchmarks, however, the main one again being the subjectivity of delivery with a diverse range of schools enforcing these standards to different degrees of effectiveness. There is also no learning outcomes or reference to the Careers Development Institutes 11-19 framework. The attention to monitoring, review, evaluation and improving careers is quite weak with no requirement for external validation of what the school records into their systems.

The Gatsby Benchmarks nonetheless is an area which could articulate the different career paths in cybersecurity, not only technical but strategy, policy and human aspect areas. As Ruth Davis of BT puts it: *'people do not understand what a career in cybersecurity is or what they need to do to get there in the same way in which someone at secondary school will understand what the career path is to become a doctor or a lawyer'* [14].

Functional Skills: The functional skills standards (noted in figure 9) were designed so student could develop the flexible English, mathematics and ICT skills needed in employment. 'Functionality' refers to the ability to apply skills to solve problems in work or society. They are not about the basics of reading, writing, arithmetic and using ICT - but the acquisition of these skills are needed to get to the higher skills.

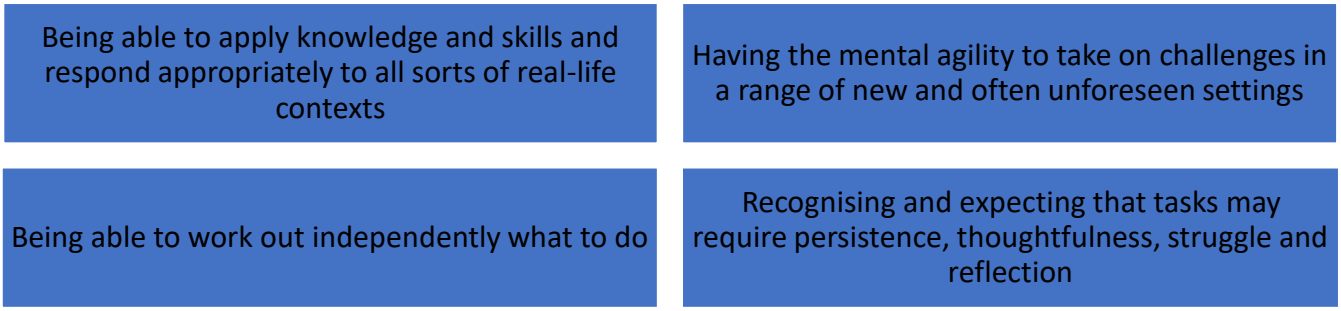

Figure 9: The Functional Skills [3]

The idea of these skills is that they are integrated into and across the curriculum into all areas of study. To be effective it is noted they need to be relevant to the subject being studies and applicable in the real world. These skills relate to the attributes frequently possessed by cyber security specialists, including mental dexterity, problem solving and logic [14]. Training these skill sets would therefore be beneficial for the workforce of the future who is likely to come across technology more frequently and would therefore be able to adapt to changing working practices more flexibly.

I have seen this framework being used at an extremely high level within a secondary school setting in a double mathematics lesson. Pupils were given logic puzzles related to the topic being taught for them to solve, there being many different ways of completing the task. Pupils were first set the task independently with the class then coming together to discuss all possible options later on. In the same lesson fractions were applied to the real world through a variety of scenarios including shop sales and income tax. It was noted this was not only relevant to the lesson but also bought in the real world including the higher level thinking skills noted in figure 9.

Once again what is of concern and a maybe act as a barrier to these higher skills for some pupils is the ability to role this out across all UK schools to a high standard. It takes a highly qualified teacher to seamlessly integrate this into a lesson without any guidance but for a box of four sentences to work with. Once again examples of lesson plans that can be downloaded from an open source would be useful for teachers to get up to speed on this.

Conclusions:

On looking school cybersecurity it has been found to be a complex moving target with lots of stakeholders in play. Combating the cybersecurity challenge seems to mandate a hierarchical approach with efforts and collaborative input needed from the individual (pupil and teacher), schools, companies and the government. With these areas working together, however, it will to help build a layer of defence to reduce exposure to cyber incidents in the UK of the present and the future [5].

The national curriculum is essential to deliver skills needed for the next generation of cybersecurity specialists. However, it seems to be that currently the idea is to keep this broadly untouched in terms of content with the cybersecurity overlay being threaded subtly through subjects and added within careers or higher level 'functional skills' training.

The benefits of integrating into relevant subjects (such as business studies or law) would make non-technical cyber skills accessible to more people and get increased functional as opposed to technical skills coming out of schools. The downside would be teachers needing to be trained in cybersecurity in order that the learnings imparted to pupils are relevant and exciting – not just something to be ticked off a list forced on teachers to complete by the government.

As a previous teacher I am all for keeping the national curriculum from having too many changes given the roller coaster of alterations over recent years bought on by government reshuffles. Although embedding cyber security in relevant subjects 'from primary to postgraduate level' is a stated aim of the 2016 NCSS [5], it has been noted 'the jury is out' on this issue among educationalists [14].

The government has stated the objective of identify and bring on talent earlier in education and develop clearer routes into cyber security roles [5]. The right level and blend of cyber expertise and skills are needed across the workforce for a secure digital economy which starts at school [7]. There are lots of extra-curricular programs that have proven effective so far which could benefit from being scaled up [14], including those to help reduce gender bias noted in various studies [1].

It has been noted that moving cybersecurity education earlier helps children have basic cyber safety when they get their first smart phone or ipad. There is a multitude of information and training available but this needs to be more joined up as the cybersecurity in schools program can be confusing and overwhelming or hard to find.

The teaching profession would greatly benefit from not only the detailed guidance provided by the government but also by practical ways to implement these learning – especially given teachers are time pressured and maybe uncomfortable teaching cyber skills. This could be in the form of lesson plans adapted for white boards (or ipads) which would have a 'plug and play' ability being tailored for different topics and lengths of lesson. It was noted that a few examples of these are available online for free but they are very basic which do not encompass the 'functional skills' metrics.

Webinars for training of teachers would also be useful in this area, although it is noted some are available already mainly through the safeguarding part of teacher training [29]. In the government plans there does seem to be a lot of emphasis on teachers increasing their skills and knowledge, however specific training examples are not provided. Given teachers are already extremely busy with lots of pressures on their time the government need to be mindful of their workloads. Anything to reduce pressure on the profession would

be welcomed which could be provided through webinars, pre-prepared lesson plans and one place in which to find all the overwhelming amounts of information in this area.

Active support to help to manage schools with their cyber defences was noticeable absent - which is also the situation in the general population. There is no official safety net in place to support schools who fall victim to cyberattacks with a lighter supporting infrastructure than areas such as physical crime, health and safety. There is no risk management for cybercrime for example which is analogous to the police force for physical crime. The situation is one in which there is a great deal of advice provided by a range of institutions and government departments, with the closest 'helping' agency being the National Cyber Security Centre, but again this is mainly an advisory body. This has been noted in literature as a way by which the government is responsibilizing the cyber security risk [4].

Further research:

In looking into cybersecurity in the state school sector other areas of investigation have presented themselves, these are noted below:

Consistency across schools: As noted throughout, there seems to be a need to ensure consistency in terms of quality (rather than individual content) across schools. Given the wide variety in Ofsted ratings across schools and even teacher ability within schools there could be a wide variety of outcomes, especially given the subjective nature of some of the guidance. It would be tragic if pupils who needed cyber safety the most were being let down by the education sector. This will always be an issue so anything which could be put into place to reduce this gap would be extremely useful.

Accessibility: There is an amazing range of out of school activities provided by the government and industry. Research into the socioeconomic classes and ethnic backgrounds of participants would be useful to ensure these are targeting a wide range of the UK population. Exclusion from these programs due to a lack of funds to get to events or logistics problems due to personal circumstances could be investigated and rectified if found.

Online resources for teachers: Teachers having open source lesson plans to draw upon for cyber safety education which is given in very detailed guidance but maybe hard to access if time short or difficult to interpret for a non-specialist. This would also be an excellent resource to have if the government were to push out cybersecurity education as a blanket across subjects. If say the business studies teacher had lesson plans produced by an expert in cybersecurity for these areas which bought the area to life pupils are more likely to have an interest in this area. As noted widely by pupils on a visit to a secondary school [29] the way the teacher presents the lesson influences which subjects they have chosen to choose at GCSE options.

Online cybersecurity knowledge: In the cybersecurity profession professionals in the area of cybersecurity have collaborated to produce a Cyber Security Body of Knowledge (CyBOK) [42] which is available for free online. Something similar but at an appropriate level and accessible for both teachers and pupils would be of benefit in this area to enable self-study for those interested.

Research has noted that 10% of the UK's economic output can be linked to online learning, with over three quarters of people who use online learning say its beneficial to their mental health [43]. With two thirds of the UK workforce using online learning to help with work this is something which can be utilised in schools and can be widely implemented if initially completed by cybersecurity educational professionals.

Educate parents: Educating parents through sessions during or after school in cyber hygiene or even running courses in which parents can gain a qualification in a technical subject will make them more confident in helping children with their work. This has been done at varying degrees of success in many schools with English and mathematics courses.

Through Parentmail (an online communication tool for schools) [27] I was informed of such a session cyber safety session run for parents for the benefit of their children. This was run by collaboration of industry (Vodaphone) and the local council (Runnymede Borough Council). Sessions such as these will not only help protect children through increase parent knowledge of dangers and preventative measures available online but also increase the resilience of the UK to cyberattacks as per the requirement of the NCSS [5]. Again, attendance at such courses would be useful to note to ensure a wide range of the population is covered by these events.

Female Participation: At a Global level, women comprise only 11% of the cybersecurity workforce. Statistics for computer science GCSE and A-Level were noted at 20% and 9% respectively in 2017 [35, 14]. Initiatives such as CyberGirls and adding coding to the curriculum from early in primary school are thought to help in raising this number but given such a low participation, further ideas need to be found to raise these numbers.

A figurehead: Various participant in a government study noted maybe a role model or figurehead would benefit the cybersecurity industry to increase visibility and attractiveness, analogous to Professor Brian Cox for physics or Sir James Dyson for engineering. With Ruth Davis of BT stressing the importance of identifying someone under-represented groups could identify with this could raise awareness and enthusiasm for the subject [14].

Final Note:

It seems reasonable that the people with the required skills are employed within the cyber security sector. This includes the ability to quickly learn, adapt and find patterns within information. Within the UK job market though cv sorting processes and interviewing techniques may overlook some of the people who are suited to cybersecurity work – or put them off applying in the first place. If people have picked up cyber skills by other means than formal education this needs to be acknowledged.

It is progress that there is now an institute of information security but hopefully this will not be a way of excluding people who do not have this qualification. As noted below in general, but would apply equally well to cybersecurity roles:

‘It’s time to radically rethink how we measure professional skills - so we can stop obsessing over qualifications, and focus on developing ability instead.’
Polly Mackenzie, Chief Executive, Demos [43]

Acronyms:

ASD: Autistic Spectrum Disorder
CyBOK: Cyber Security Body of Knowledge
DDoS: Distributed Denial of Service
DCMS: Department for Digital, Culture, Media and Sport
EYFS: Early Years Foundation Stage
GDPR: General Data Protection Regulations
ICT: Information Communication Technology
LGfL: London Grid for Learning
NCSC: National Cyber Security Centre
NCSS: National Cyber Security Strategy
OECD: Organisation for Economic Co-operation and Development
Ofsted: Office for Standards in Education
PSHE: Personal and Social Health Education
STEM: Science, Technology, Engineering and Mathematics

References:

[1] Renaud K., Flowerday S., Warkentin M., Cockshott P., Orgeron C. (2018). Is the responsibilization of the cyber security risk reasonable and judicious? Science Direct, [online] Available at: https://reader.elsevier.com/reader/sd/pii/S0167404818303262?token=60557088375C199DB30189DF42FB2E1FE6608ECB1DFA7853D5566AED28FC8F6E818AD9C6AED14FDE807520FF3B70CDCE [Accessed 26 Feb. 2020].

[2] Manyika J., Lund S., Chui M., Bughin J., Woetzel J., Batra P., Ko R. and Sanghvi S. (2017). Jobs lost, jobs gained: What the future of work will mean for jobs, skills, and wages. Mckinsey. [online] Available at: https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages [Accessed 26. Feb 2020].

[3] (2020) Chartered institute of information security. Iisp. [online] Available at: https://www.iisp.org [Accessed 26 Feb. 2020].

[4] (2019). UK Cyber-security skills gap ‘at breaking point’. Net imperative, [online] Available at: http://www.netimperative.com/2019/11/uk-cyber-security-skills-gap-at-breaking-point/ [Accessed 26 Feb. 2020].

[5] (2019) Initial National Cyber Security Strategy: increasing the UK’s cyber security capability – a call for views. [online] Available at: https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views [Accessed 26 Feb. 2020].

[6] Coughlan S. (2019). England’s schools ‘worst for cyber-bullying’. BBC. [online] Available at: https://www.bbc.co.uk/news/education-48692953 [Accessed 26. Feb 2020].

[7] Contact with [ ] Preschool in a parent capacity

[8] Contact with [ ] Infant School in a parent capacity

[9] Contact with [ ] Infant School in a parent capacity

[10] Contact with [ ] High School in a Governor Role (Education, Curriculum and Outcomes)

[11] (2019) Key UK education statistics. Besa. [online] Available at: https://www.besa.org.uk/key-uk-education-statistics/ [Accessed 26 Feb. 2020].

[12] Muncaster P. (2019). Pupils Flagged as Cyber Threat to UK Schools. Infosecurity Magazine. [online] Available at: https://www.infosecurity-magazine.com/news/pupils-flagged-as-cyber-threat-to/ [Accessed 26 Feb. 2020].

[13] (2019) Clowne's Heritage High School closes early for summer after IT systems attacked. PeakFM. [online] Available at: https://www.peakfm.co.uk/news/local/clownes-heritage-high-school-closes-early-for-summer-after-it-systems-attacked/ [Accessed 26 Feb. 2020].

[14] (2019) GCSE coursework lost in cyber attack on Birdport school. BBC. [online] Available at: https://www.bbc.co.uk/news/uk-england-dorset-47551331 [Accessed 26 Feb. 2020].

[15] (2019) The increasing need for cybersecurity in the education sector. Dealer Support. [online] Available at: https://dealersupport.co.uk/the-increasing-need-for-cybersecurity-in-the-education-sector/ [Accessed 26 Feb. 2020].

[16] Keer M. (2019) Cybersecurity – Going back to school. NCSC and LGfL. [online] Available at: https://www.ncsc.gov.uk/blog-post/cyber-security-going-back-to-school [Accessed 26 Feb. 2020].

[17] Aston C. (2018) Cyber attacks hit a fifth of schools and colleges. IT governance. [online] Available at: https://www.itgovernance.co.uk/blog/cyber-attacks-hit-a-fifth-of-schools-and-colleges [Accessed 26 Feb. 2020].

[18] (2018) Gatsby Benchmarks. The Careers & Enterprise Company. [online] Available at: https://www.careersandenterprise.co.uk/schools-colleges/gatsby-benchmarks [Accessed 26 Feb. 2020].

[19] (2019) Regulation for the Forth Industrial Revolution. BEIS. [online] Available at: https://www.gov.uk/government/publications/regulation-for-the-fourth-industrial-revolution/regulation-for-the-fourth-industrial-revolution [Accessed 26 Feb. 2020].

[20] Center, I., Blignaut, R., Renaud, K., Venter, A. (2019). Cyber security education is as essential as "the three R's". Heliyon, [online] Available at: https://reader.elsevier.com/reader/sd/pii/S2405844019365144?token=C53CA5F41535BD44C7207D6E9F4FE7AE06FF3D1E92540833801C4377B894A2A68AEAAB232E244F1423FB6ABDA001C6DC [Accessed 26 Feb. 2020].

[21] (2014) National curriculum in England. HM Government. [online] Available at: https://www.gov.uk/government/collections/national-curriculum [Accessed 26 Feb. 2020].

[22] (2018) Revised GCSE and equivalent results in England: (2016 to 2017). Department for Education. [online] Available at: https://www.gov.uk/government/statistics/revised-gcse-and-equivalent-results-in-england-2016-to-2017 [Accessed 26 Feb. 2020].

[23] (2017) A level and other 16 to 18 results: (2016 to 2017) - provisional. Department for Education. [online] Available at: https://www.gov.uk/government/statistics/a-level-and-other-16-to-18-results-2016-to-2017-provisional [Accessed 26 Feb. 2020].

[24] (2018) Analysis of GCSE STEM entries and results. Wise. [online] Available at: https://www.wisecampaign.org.uk/statistics/analysis-of-gcse-stem-entries-and-results/ [Accessed 26 Feb. 2020].

[25] (2016) National Cyber Security Strategy 2016-2021. HM Government. [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf [Accessed 26 Feb 2020].

[26] (2018) Joint Committee on the National Security Strategy – Oral Evidence. [online] Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/cyber-security-critical-national-infrastructure/oral/83327.pdf [Accessed 26 Feb. 2020].

[27] The European handbook for teaching privacy and data protection at school. [online] Available at: http://arcades-project.eu/images/pdf/arcades_teaching_handbook_final_EN.pdf [Accessed 26 Feb. 2020].

[28] (2019) Initial National Cyber Security Skills Strategy: Increasing the UK's cyber security capability – a call for views. DCMS. [online] Available at: https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views [Accessed 26 Feb. 2020].

[29] (2018) Serious and Organised Crime Strategy. HM Government. [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752850/SOC-2018-web.pdf [Accessed 26 Feb. 2020].

[30] Rasberry Pi Foundation. [online] Available at: https://www.raspberrypi.org/about/ [Accessed 26 Feb. 2020].

[31] (2016) Chancellors speech: launching the National Cyber Security Strategy. Uk Government. [online] Available at: https://www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy [Accessed 26 Feb. 2020].

[32] 10 steps to better cybersecurity and safeguarding for schools. Beaming. [online] Available at: https://www.beaming.co.uk/insights/cybersecurity-safeguarding-approach-schools/ [Accessed 26 Feb. 2020].

[33] Anti-Bullying Alliance. [online] Available at: https://www.anti-bullyingalliance.org.uk/tools-information/all-about-bullying/curriculum [Accessed 26 Feb. 2020].

[34] (2019) Teaching online safety in schools. Department for Education. [online] Available at: https://www.gov.uk/government/publications/teaching-online-safety-in-schools?utm_source=ABA%20Member%20List&utm_campaign=ed5438dae6-EMAIL_CAMPAIGN_2018_09_04_02_00_COPY_01&utm_medium=email&utm_term=0_cd96ad603f-ed5438dae6-321385141&mc_cid=ed5438dae6&mc_eid=8df2fa7897 [Accessed 26 Feb. 2020].

[35] (2018) Education for a connected world. UK council for internet safety. [online] Available at: https://www.gov.uk/government/publications/education-for-a-connected-world [Accessed 26 Feb. 2020].

[36] (2019) Functional Skills standards curriculum. Education & Training Foundation. [online] Available at: https://toolkits.excellencegateway.org.uk/functional-skills-starter-kit/section-3-developing-effective-practice/functional-skills-standards-and-curriculum [Accessed 26 Feb. 2020].

[37] Pedley D., McHenry D., Motha H., Navin Shah J. (2018). Understanding the UK cyber security skills labour market. Ipsos Mori. [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767422/Understanding_the_UK_cyber_security_skills_labour_market.pdf [Accessed 26 Feb. 2020].

[38] (2019) CyBOK. [online] Available at: https://www.cybok.org/media/downloads/CyBOK_version_1.0_YMKBy7a.pdf [Accessed 26 Feb. 2020].

[39] Mackenzie P. (2020). The Learning Curve: How the UK is harnessing the potential of online learning. Demos. [online] Available at: https://demos.co.uk/project/the-learning-curve/?mc_cid=a22226e7c4&mc_eid=e143aa1621 [Accessed 26 Feb. 2020].