Briefing on web monitoring and keyword logging software in schools

"Safeguarding of children and of individuals at risk" government proposed amendment in the DP Bill

1. Summary

1.1 We ask you to reject the new clauses 85, 116 and 117 sought in Schedule 1, 8 and 10, outlined on pages 8, 23 and 29[1]. Data protection law already adequately enables safeguarding practices of safe, fair and lawful transfer of personal data, including sensitive data, under public interest or legitimate interests or crime. If it does not, then there is something wrong with policy and practice, not Data Protection law. Where guidance on responsibilities is needed, it should fall into a statutory code of practice under the ICO. There are already exemptions in the Bill for education, health and child abuse. New conditions for processing which read akin to exemptions from rights, should be rejected at this late stage without significant scrutiny.

1.2 The amendments introduce new 'safeguarding' clauses and would encompass data transfers done in the name of "safeguarding in schools" policy introduced through Statutory guidance in September 2016[2] without public debate, and **causes young people harm, and prevents their full freedom to develop. It restricts their freedom of speech, participation, and flourishing. Where defined necessary and proportionate purposes are lawful today, why is another new condition for processing that is not already in current data protection law necessary. Question: Is current practice therefore not lawful, and in what circumstances are any of these new conditions for processing needed?**

1.3 These amendments could establish conditions for processing with broad interferences with data transfer in communications, excessive sharing of sensitive categories of personal data, correspondence, photos, webcam, location, content surveillance; and the onward distribution of children's sensitive data without purpose limitation, or safeguards -- in conflict with data protection by design and default (GDR Art 25) that *"In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."*.

1.4 To reduce harm to children, data transfers in new safeguarding policy and practice introduced in September 2016 need reviewed and changed, not embedded in statute and made exempt from the safeguards of Data Protection law, under special pleading for acceptance of currently invasive practices, where it is not clear today that it is lawful.

1.5 Safeguarding practice in schools currently imposes 24/7 365 day a year web surveillance on many children, and full time online surveillance in schools for nearly every child in England.

1.6 The proposed clause 2(a-c) processing carried out without the consent of the subject is

[1] Bill amendments March 8, 2018 https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/amend/data_rm_pbc_0308.pdf
[2] Safeguarding in Schools p17 para 67. Plus Annex C
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550511/Keeping_children_safe_in_education.pdf

dependent on acceptance the balance should be in favour of processing without informed consent. Children cannot consent under data protection law anyway to such processing, due to public authority power imbalance. Parents indicate in a recent independent survey[3] of 1,004 parents that children and guardians should be informed how keyword logging works. Children want to understand how their data are processed and restore power imbalances, outlined for example in, *The Internet on our own Terms: how children and young people deliberated about their digital rights* (Jan 2017) (Research by Coleman, S., Pothong, K., Vallejos Perez, E., and Koene, A. supported by 5Rights, ESRC, Horizon, University of Leeds and University of Nottingham).

1.7 Article 5 of Directive 2002/58 is devoted to the confidentiality of communications; Article 5(1) provides: 'Member States shall ensure the confidentiality of communications and the related traffic data [...] **shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned**...' and, that **the 'law' must, in effect, be 'adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct', to 'foresee its consequences for him[4]'**, 'to foresee, **to a degree that is reasonable in the circumstances, the consequences which a given action may entail'**.[5]

1.8 Interception of communications transmitted via a private telecommunications system was found not in accordance with the law in Taylor-Sabori v the United Kingdom. In Rotaru v. Romania the ECtHR found a violation of Article 8 of the ECHR due to the lack of limitation on collection and archiving surveillance information. **The depth of privacy invasion caused by current policy is not proportionate to the aim pursued, it is not necessary in a democratic society**, (Leander v Sweden, ECtHR March 1987) **or proportionate to a school's responsibility of personal time outside school hours**. The Internet screen recording and disclosure to an unnamed list of third parties at provider companies, inside a Multi Academy Trust, or to outside authorities including police without transparency to the child is disproportionate and without any limitation or safeguards even if at risk, similar to Peck vs United Kingdom when video disclosures by the Council were not accompanied by sufficient safeguards and they constituted a disproportionate interference with rights under Article 8.

1.9 Considering the conclusions in **the UKSC decision in Christian Institute & Others[6]** which considered sharing of information about children in Scotland, in particular the incompatibility with data protection law we believe current practices breach current Data Protection Directive (Article 15), the Human Rights Act 1998, the Charter of Fundamental Rights Articles 7 and 8, and the UNCRC[7] Article 16 (children have a right to privacy, and the law should protect them from attack on their way of life, reputation, families and home).There is interference with Article 11 of the Charter of Fundamental Rights on Freedom of Expression, "to hold opinions and to receive and impart information and ideas without interference by public authority and

[3] Survation poll of parents of children age 5-18 in state education carried out for defenddigitalme on use of pupil data in England http://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables.pdf
[4] European Court of Human Rights, judgment in *Leander v. Sweden* [1987] no. 9248/81, Series A no. 116, § 50
[5] ECHR, judgment in *Margareta and Roger Andersson v. Sweden* [1992] no.12963/87 Series A no. 226-A p.25 § 75
[6] "Named Persons" Supreme Court ruling https://www.supremecourt.uk/cases/docs/uksc-2015-0216-judgment.pdf
[7] Children are holders of all the rights in the Convention, entitled to special protection measures and, the progressive exercise of their rights http://www2.ohchr.org/english/bodies/crc/docs/AdvanceVersions/GeneralComment7Rev1.pdf

regardless of frontiers." The Children's Commissioner for England believes we are failing in our fundamental responsibility as adults to give children the tools to be agents of their own lives.[8] This processing is a gross example of this, despite packaging as in a child's best interest. No one has asked parents and children if they want this surveillance of their Internet use which is carried out at school, in the home, and outside school hours. Parents and children's views we provide, show this data transfer is excessive and unjustified intrusion.

[8] Growing up Digital Taskforce 2017 https://www.childrenscommissioner.gov.uk/publication/growing-up-digital/

Case study: Childline is a service provided by the NSPCC

The Childline webpage tells children about how web monitoring software works and proactively encourages them to use a school website in order to avoid web monitoring systems and protect the confidentiality of, "*what they are saying in a 1-2-1 counsellor chat or email with a counsellor or posting on the message boards.*

"if you need to view pages or talk to a counsellor on the Childline website, try to use a different computer that doesn't have the monitoring software installed (such as a computer in a library, internet café ***or school).***[9]*"*

The NSPCC and Childline clearly see the importance of children trusting in data privacy in order to access help. This advice can no longer hold true for children in the majority of schools in England and for the government to seek to embed this breach of children's trust is alarming.

[9] Childline (accessed March 10 2018) https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/cover-tracks/#4

2. What does current data transfer in safeguarding look like

2.1 A single paragraph in 2016 Statutory Guidance created an explosion in use of Internet monitoring software imposed by schools in -- and outside -- the classroom, without oversight or guidance what was acceptable policy. Compare the volume of just one UK provider in November 2016 in the research report carried out by Big Brother Watch[10] in which they believed Impero was used by 403 schools; and today it is installed in over 1,400 UK schools.[11]

2.2 Web monitoring software of every child's Internet use, records and monitors by default everything the child does online, and can include home use and outside school hours, where they are not always restricted to the school network, or logging into the school network is necessary for homework or use at home. Often these software are installed on personal devices, imposed as a requirement to use the phone on the school network, and installed on school Chrome Books for example, taken home to do homework, or for the summer holidays.

2.3 Typical functionality includes:

i. Web filters to prevent access to content and page blocking -- without personal data transfer

ii. Web monitoring and keyword flagging -- which does transfer personal data to third parties

- Any use of keywords in the company **libraries of up to 20,000 words create flags**
- **Alerts on individuals are sent to school administrators, authorities or police**

iii. **Webcam remote access** by administrators[12] has unclear necessary, proportionate basis.

iv. **Screen recording 24/7** of everything a child sees, creates, or types on the device.

2.4 As an example of this technology **where police are notified automatically**, SWGFL, part of RM education, offers a product RM SafetyNet. Few answers are forthcoming how it works.

"Includes RM SafetyNet and prevents access to illegal content including the IWF CAIC and Online Terror Content Access attempts are proactively monitored with unique links to Police and expert support in an emergency."

All school traffic is forced through the platform, and run against mandatory lists of content which are listed as blocked, illegal or seen in some way as harmful. School administrators, pupils and parents do not know which sites are 'flagged' and blocked and the system cannot be switched off. The content of the lists is secret. School staff and even the help centre staff for the software do not know what words trigger watchlists; flags on children's records forever.

2.5 The undefined "authorities" are notified, if someone tries to browse to one of those websites listed, but the school and teacher who knows the child may not necessarily be contacted. These flags are therefore created and can be acted upon for intervention without context or local knowledge. The lists and keywords come from a combination of three sources:

- **The Internet Watch Foundation (IWF) (illegal content)**
- **The Counter Terrorism Internet Referral Unit (CTIRU) (Prevent)**

[10] Another Brick in the Wall (p5) Big Brother Watch (2016) https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/11/Classroom-Management-Software-Another-Brick-in-the-Wall.pdf
[11] www.imperosoftware.com/uk/resources/press-releases/impero-software-announces-new-ceo-richard-fuller-sam-pemberton-moves-advisory-board-position/
[12] http://defenddigitalme.com/wp-content/uploads/2018/03/NetSupportDNA_webcamgallery.jpeg

- Categories designed by the provider (these vary from provider to provider and can contain foreign language modules.) **and include libraries of around 20,000 words** claimed to each be about the prevention of bullying, self-harm, and child protection.

3. How to measure success

3.1 The limitations of filtering and monitoring technology are clearly set out by Professor Phippen in the 2017 book, *Invisibly Bighted, The Digital Erosion of Childhood,*[13] including the inability to prevent or identify embedded imagery (for example of a social media page), peer-to-peer systems, personal networks, and simply those who are determined wto work around them. But lack of guidance and democratic discussion of monitoring children is even more concerning when it comes to interference with privacy, rights, and harm.

3.2 *"The recent draft statutory guidance on safeguarding by the Department for Education (2015) defines an expectation that schools have monitoring in place and governing body is responsible for it to be 'appropriate.'*

3.3 *[Schools] need to have appropriate filters and monitoring systems, so that no child can access harmful content via the school's IT systems and concerns can be spotted quickly. [Department for Education, 2015]*

3.4 *However there seems to be no guidance on what appropriate means aside from further guidance to ensure 'unreasonable restrictions' are not placed on what can be taught." [end quote]*

3.5 The systems are inconsistent in their approach and severity but their "success" is measured in "risks identified" and "flags". A change of system provider from Bloxx to Smoothwall in a school resulted in staff raising concerns with us at defenddigitalme in January 2018 because the new software,"*created an enormous spike"* in search terms flagged, without any change in one school's student population or, the staff believe, a sudden increase in risk levels. **Searches involving cliffs and black rhinos earned children flags as potential suicide risk and gang member respectively. These are simply wrong, but the staff cannot remove the flags.**

3.6 *"If a keyword is triggered which the school deems to be a false match, a note can be added allowing the reviewer to explain why.*" [14] **It is impossible for children to get these errors removed. They can be held on record indefinitely, shared with Prevent and police and show up in statistics.** Companies have no incentive to lower their "success rate" of events.

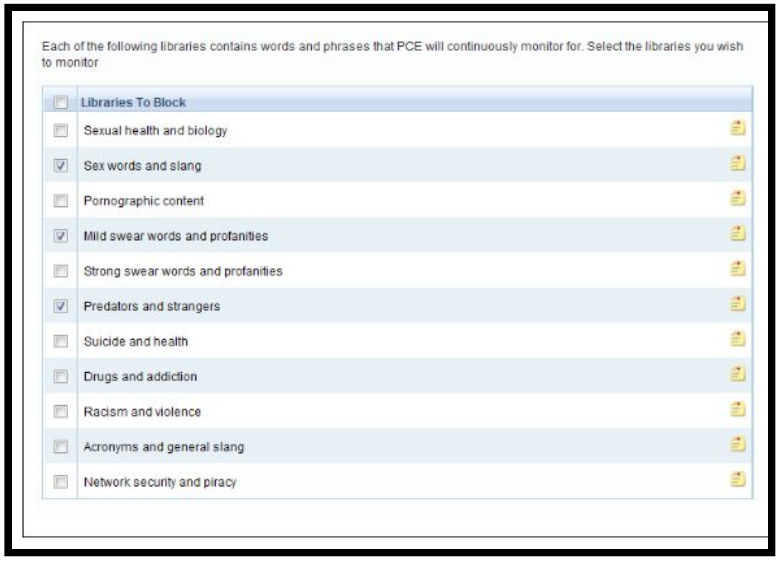
3.7 **A measure of harm done and harm which is unmeasured needs an independent review. PCE:** The desktop libraries contain words and phrases that relate to different forms of unacceptable use. The libraries are split into different themes. The harm from the chilling effect of a child unable to use the Internet at home with parental monitoring, and knowing that looking up sexual health or sexuality on a website at school will create a flag to a member of staff and/or an external third party should not be underestimated. **There has been no**

[13] *Invisibly Bighted, The Digital Erosion of Childhood,(2017) r*esearch by Leaton Gray, S. Dr and Phippen, A.Prof. (p92)
[14] NetSupport DNA Education http://www.netsupportdna.com/education/features.asp#safeguarding

independent assessment of the volume of these types of scenarios and we cannot measure that which has not happened, **the confidential searches for support unable to be done.**

3.8 There is evidence from talking to children in research by academics Dr Leaton and Professor Phippen, that when subjected to invasive monitoring, children are changing their behaviours to work around the policies in order to maintain their privacy. "Images were not stored on phones but immediately uploaded to cloud storage. This is not because they were doing anything illegal but simply because young people would rather their parents did not see everything they want to search for.[15] Many pupils reported deleting anything medical and body related *(usually involving them trying to find out anything about puberty and sex) from their browsing history"*. >> Oservation of their digital content has a chilling effect on children.

3.9 There is evidence from our discussions with school staff that children have learned some of what will trigger the keywords and use this as a prank tool or to bully and harass each other out of the classroom using staff intervention as the vehicle. By looking up content while a peer is logged in to a computer but away from the desk, a fellow child can search for something that gets the logged-in child hauled before staff and in one case, the safeguarding panel.



4. Company backgrounds and questions of implementation

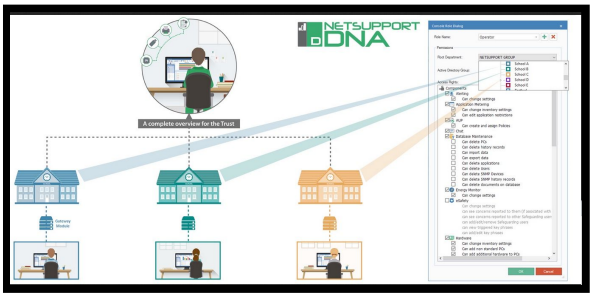
4.1 **Impero Education Pro** is already being used on over 1.6 million workstations in schools in 181 local authorities across the UK. In contrast with some council run systems, Impero Software is one of the leading commercial UK providers, and backed by Connection Capital,[16] a leading private equity investor in the UK SME market and independent UK bank BLME. **BLME[17] is the largest wholly Islamic bank in Europe specialising in Wealth**

[15] Invisibly Bighted, The Digital Erosion of Childhood, Leaton Gray, S. and Phippen, A. (p56) 2017 UCL ISBN 978-1-78277-050-3
[16] Buyout of Impero Software https://www.imperosoftware.com/uk/resources/press-releases/connection-capital-completes-10m-management-buy-leading-e-safety-classroom-network-user-management-software-provider-impero/
[17] About BLME https://www.blme.com/about-blme/

Management with complementary Real Estate, Lease Finance and Trade Finance offerings.

4.2 **Technical issues in Impero Education Pro**, it was reported in 2015 in the Guardian[18], that The software can be exploited to cause remote command execution on every client. Security researchers warned the company twice of serious flaws but the company reportedly failed to fix them and responded, *"with a legal threat to a security researcher that highlighted a serious security flaw in your software is bizarre and shows utter disregard for customers."*

4.3 **NetDNA support.** When a safeguarding keyword is copied, typed or searched for across the network, **NetSupport DNA can now remote activate webcams to capture an image of the child** – in addition to providing a recording and screenshot of the trigger word / content.



4.4 Safeguarding staff can flag 'at risk' students on the system so they can be easily identified and tracked as an extra layer of support. A dynamic group is also provided so all vulnerable students across the school can be seen from a single view. However, in an attempt to create access to and lists of people to see and protect, it creates ways to view a vulnerable child, and honeypots of vulnerable students anyone with access to the group single view could misuse for grooming, blackmail or other purposes. We are concerned this is open to misuse. [fig 1]and far from "making the UK the safest place to go online" actually increases risk for children.

4.5 **Web monitoring of children and staff 24/7, 365 days a year including at home in personal space and in private time**. Communications Committee, 11 October 2016, Mark Donkersley, Managing Director, **e-Safe Systems Limited,** told the Committee[19]:

4.6 *"Bearing in mind we are doing this throughout the year, the behaviours we detect are not confined to the school bell starting in the morning and ringing in the afternoon, clearly; it is* ***24/7 and it is every day of the year.*** *Lots of our incidents are escalated through activity on evenings, weekends and school holidays. Invariably, although the volume decreases, for example, during the six-week school holiday in the UK, the proportion of incidents which are very serious during that period is much higher."* They are tracking at home, all hours. Who is using the laptop, or device, may not be the child whose named account gets flagged.

[18] https://www.theguardian.com/technology/2015/jul/14/security-flaw-found-in-school-internet-monitoring-software
[19]http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/oral/41158.html

4.7 **Freedom-of-Information requests** collected between December 2016 and April 2017 from 190 schools in England and 30 schools in Northern ireland for the defenddigitalme report *The State of Data: New rights and Responsibilities* **show 50% of schools that replied, enable this web monitoring software on BYOD (Bring your own [private mobile] device).**

4.8 Whether the school monitors the pupil's Internet use at home or not is usually only when connected to the school network remotely, and/or using school property, but can also include personal devices if they have been used in school and installed. Answers include,

"Yes if you log into your profile, no if you use your personal data eg 4G.

"Not currently, this is something which we are looking at in the next update. The solution was only implemented in November.

"Monitoring software is used on school premises and when a device accesses the school network remotely.

"Yes if ever academy property used".

"Theoretically yes, in practice no. The solution would monitor usage on college devices wherever they are used. However, devices are not given to students to take home.

"The internet history is recorded from the device and stored on the Lightspeed server for 6 months but can be extended.

5. Prevent Programme and Channel

5.1 In 2015/16 according to the Prevent Programme statistical bulletin[20], a total of 7,631 individuals were subject to a referral due to concerns that they were vulnerable to being drawn into terrorism. **The education sector made the most referrals (2,539) accounting for 33%**, followed by the police (2,377) accounting for 31% of referrals.

5.2 In 2015/16, of 7,631 individuals referred, the majority (4,274; 56%) were aged 20 years or under. **Individuals 2015/16 from the education sector had the youngest median age (14).**

5.3 Of the 7,631individuals referred in 2015/16: 2,766 **(36%) left the process requiring no Further action** 3,793 (50 %) were signposted to alternative services, **1,072 (14%) were deemed suitable, through preliminary assessment, to be discussed at a Channel panel.**

5.4 **Rights Watch (UK) and Liberty are concerned that**, despite broad policy statements of compliance with data protection and privacy rights, the operation of the Prevent strategy and the Channel programme on the ground does not demonstrate due respect for personal information and privacy. "*From the case studies considered by RW(UK) in its 2016 report, 'Preventing Education?', it appears local authorities, schools, and police authorities may be operating some system of data collection and sharing which records a child's interaction with the Prevent strategy or the Channel programme. This could include formal referrals, informal information and events such as a police visit to a child's home. RW(UK) and Liberty have*

[20] Individuals referred to and supported through the Prevent Programme, April 2015 to March 2016 http://defenddigitalme.com/wp-content/uploads/2018/03/individuals-referred-supported-prevent-programme-apr2015-mar2016.pdf

significant concerns about the rigour and compliance of such a system of data collection with both the specific requirements of current data protection laws and the Human Rights Act".

5.5 **CRIN (Child Rights International Network) told us, "***The Channel programme operates through panels, led by a representative of the police (the Channel Police Practitioner) and can include professionals from education, social work, immigration, housing and health services. Each panel is formed at the discretion of individual local authorities, and so their size and make up vary significantly across the country ...there is a chronic lack of transparency about the way that information is collected and fed into this process, including within schools."*

5.6 **CRIN has used freedom of information requests in an attempt to find out the ways that schools are using filtering and monitoring programs to detect signs of "radicalisation" in students. "***CRIN submitted 61 requests to schools across a London Borough to ask what filtering and monitoring programs were installed on school ICT equipment for the purposes of detecting signs of "radicalisation", information about how the software worked and how many students had been flagged up by the software. None of the schools provided detailed information and a common response was that their filtering software was operated by a public-private partnership that is not subject to the Freedom of Information Act."*

5.7 CRIN told us that, "*without a clear picture of what information schools, or private companies working on behalf of schools, are collecting and where it is held, it is impossible to assess the adequacy of mechanisms to protect the data of children. The outsourcing of services to the private sector has also has extended the number of bodies holding children's data, while limiting the potential for independent scrutiny."*

6. Parents views show that they want transparency and rights

Responses from 1,004 parents surveyed by Survation online between February 17-20, 2018[21]

6.1 Parents were asked about getting consent for this process. They were not asked *if* they support the use of Internet Monitoring software. Parents were asked only, if their school uses it to the best of their knowledge and if so, if parents should be asked for consent to do this and whether they believe they, and children, should be informed what the watchlists contain.

6.2 Given the low levels of trust indicated in the question of third-parties parents felt they would trust to use their child's data appropriately, and the high percentages that want to be informed of the consequences of keywords being searched for, then we think numbers on consent probably indicate some who disagree it should happen at all. **i.e some parents did not agree that consent should be required for Internet web monitoring, because they do not agree it should happen at all -- with or without -- consent. More research needs done. It is clear is that parents believe the keywords and consequences should be transparent and foreseeable. This amendment prejudices that, embedding current practice.**

6.3

Would you say that the current amount of control you have over which apps and online services your child is signed up to by the school (your child's digital footprint) is:	
Sufficient	50%

[21] See also footnote 3 http://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables.pdf

Insufficient	28%
Don't know	22%

6.4 **Parents were asked, does your child's school use Internet Monitoring and keylogging software (software that records children's Internet use at school)? Many do not know.**

The school uses this	The school does not use this	Don't know
46%	17%	37%

6.5

To your knowledge, is the Internet Monitoring software used by the school able to do any of the following? Please select all that apply.	
Record children's images through a webcam	14 %
Capture the screen as seen by the child	25 %
Log children's Internet search terms and create flags based on keywords	55%
None of the above	5%
Don't know	28%

6.6 Key logging software at school captures children's Internet search terms. Some systems flag up to 20,000 different words and phrases. To what extent do you agree or disagree with the following statements? **Today's opaque data practices are considered to be unacceptable.**

	Agree	Neither agree nor disagree	Disagree	Don't know
Parents should be informed of which keywords get flagged	84%	11%	4%	1%
Parents should be informed of what the consequences are if these keywords are searched for	86%	11%	2%	1%
Children should be informed of which keywords get flagged	69%	18%	12%	2%
Children should be informed of what the consequences are if these keywords are searched for	86%	11%	2%	1%

6.7 On a scale from 0 to 10, to what extent do you agree or disagree that **schools should get parental consent to be able to use each of the following? We believe this 'disagree that consent should be asked for' hides some who feel monitoring should not happen at all.**

	0-4 (disagree)	5	6-10 (agree)
Internet Monitoring software that can be run remotely at home in the evenings or during school holidays	**32%**	**15%**	**53%**

Internet Monitoring software that can record children's Internet screen use in school at all times	**22%**	**14%**	**64%**
Internet Monitoring software that can record children's images through the webcam	**34%**	**13%**	**53%**

6.8 46% were not offered any choice at all to have these invasive technologies imposed on their children. And while 54% said they were asked for consent we know that this is not a valid consent process, because there is no explanation given how it works, what data are collected, viewed or sent to whom and parents and children are often required to agree or feel compelled to accept, because there is no option offered to refuse. The amendment embeds not asking for consent as the acceptable practice in all circumstances, rather than narrow where necessary.

7. School and staff evidence

7.1 Evidence from 4,507 of 6,950 schools using the SWGfL tools who carried out e-safety self-reviews, using the 360 Degree Safe tool in analysis carried out by Andy Phippen, Plymouth University[22], shows that school staff are not equipped to deal with or challenge the outcomes from these technology. Lack of capability and training, does not absolve staff of accountability for the data management responsibilities that occur under their control.

7.2 *"However perhaps even more concerning is that the two weakest aspects are those upon which a school would be most reliant on understanding the nature of data protection and safeguarding within the school setting. If both staff and governor knowledge are poor (and in both cases averages are below 'basic' practice, indicating that a large number of establishments do not have either in place) there is little likelihood that the complex issues around data protection or safeguarding are well understood, and* ***an effective challenge to senior management on these matters certainly cannot exist."*** Mistakes go unchallenged.

7.3 We also asked IT staff in 35 schools about the use of this software and the "consent" contracts used. These are school-pupil-parent agreements which are ostensibly "consensual" contracts on how the child will use the Internet in and often outside school, with regards acceptable behaviours. They often contain a single line which says, 'I understand my online use will be monitored.' There is no explanation given what this means, how much personal data will be collected, or the surveillance that ensues. There is no explanation given of the consequences of these policies. They are invalid. Parents and children sign not wanting to be seen as "difficult."

7.4 Sample survey of 35 school IT staff with data protection responsibility [Link to responses].

7.5 In December 2016 Freedom of Information requests (FOIRs) were sent out to 216 secondary schools in Northern Ireland, Wales and England. **103 (47%) schools answered the Freedom of Information request. Based on only those responses and the 47% response rate, 59 schools (57%) used a biometric system, 20 of those schools (37%) used biometrics for more than one application.**

91% of the 59 schools used biometrics for canteen,

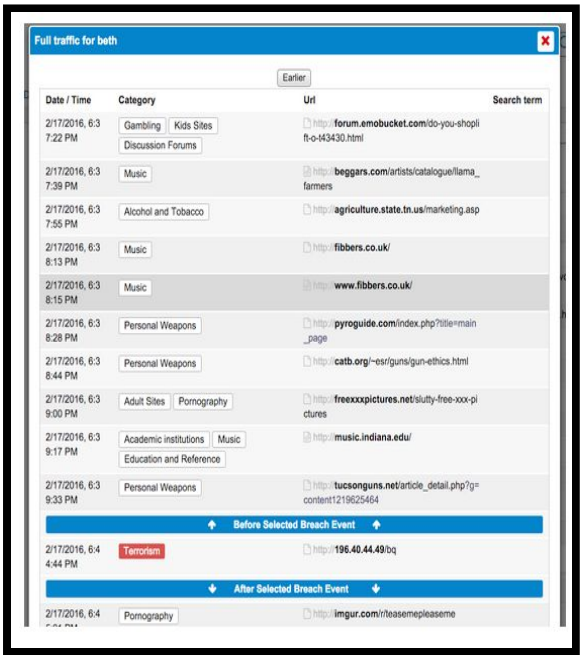
[22] Invisibly Bighted, The digital erosion of childhood, Leaton Gray, S. and Phippen, A. (p56)

13.5 % used biometrics for the school library
13.5 % used biometrics for registration
22% used for other purposes (printer, copier, door access, school gate, laptop, school trips)

These figures are likely to be a low indication of how many schools use biometric systems certainly at higher overall rates in larger and in secondary schools.

8. Appendix list of commonly used monitoring software in UK

- AB Tutor
- Bloxx
- C2K to school (Northern Ireland).
- Impero
- Fortiguard Firewall
- iTalc / Veyon
- LANschool/Lenovo
- Lightspeed Rocket
- NetSupport DNA
- Securus
- Policy Central Enterprise
- SWFGfl
- Smoothwall UTM
- Viglen
- Websense Cloud



About defenddigitalme and what we do
We are a non partisan civil society organisation. We campaign for safe, transparent and fair use of personal confidential data across the education sector in England. We are funded 2017-18 through a single annual grant from the Joseph Rowntree Reform Trust Ltd.

defenddigitalme welcomes the proposed amendment to the Data Protection Bill for a Statutory Code of Practice in Education and asks for your support. We provide the results of a recent national survey.

Survation[1] polled 1,004 parents of children aged 5-18 in state education in England on behalf of defenddigitalme between 17th-20th February.

Only half (50%) of parents polled said they have sufficient control of their child's digital footprint in school.

When asked what types of systems their child's school uses, over half (53%) of parents polled said their child's school uses closed circuit or surveillance cameras, while slightly less than half (46%) said they believe Internet Monitoring or keylogging software is used. A quarter (25%) of parents said their child's school uses biometric technology such as fingerprints, retinal scans, palm scans, or facial image recognition.

When asked how often they were told if their child's personal data will be stored or transferred to third-party organisations through a school administration software or an online learning service, only 31% of parents said they were always informed of this. 23% said they were never informed of this while 10% of parents replied, "Don't know." Personal data was defined as "any information that can be used to identify a child".

Significant populations answered they '*did not know*' to several questions how their children's personal data are used from school. As many as one in four (24%) parents said they do not know if their child has been signed up to systems using personal data. Defenddigitalme believes this is reflected in low figures of understanding how data are used, compared with schools' responses to FOI on use of these systems, which reflect as many as 70% using web monitoring and keylogging software, including 50% for personal devices, and 100% of schools are required to submit children's personal data in the school census to the DfE.

The majority of parents (69%) polled said they had not been informed that the Department for Education (DfE) may give their child's personal data to third parties, while only 31% said they had been informed of this. Almost 4 in 5 (79%) said, if they had the opportunity, they would choose to see their child's named record in the Database. The DfE refuses this subject access right today, while journalists[2] and commercial businesses are regularly[3] given children's identifying data sent out to their settings, and "*can track students wherever they go in England*"[4] outwith DfE oversight and without fair processing to parents and children.

Survation also used a 0 to 10 scale to ask whether parents believed that parental consent should be required for school's to be able to pass children's data to the Department for Education. As many as two in three (60%) gave a score of 7 or higher, thus indicating that parental consent should be required in order to pass this information on. *For children with special educational needs or a disability*, 81% said parental consent should be required to share this data with third parties such as researchers and commercial companies.

Additionally, over a third (38%) of those who said their child's school uses biometric technology said they were not offered a choice of whether to use this system or not and 50% have not been informed how long the fingerprints or other biometric data are retained for, or when they will be destroyed — despite the Protection of Freedoms Act 2012 requiring parental consent, and an alternative to be on offer, showing that practical guidance is needed to help schools understand how to implement the legislation.

We are happy to answer any questions you may have.

Jen Persson
Director, defenddigitalme
tel 07510 889833 email jen@defenddigitalme.com

---

1 Survation polled 1,004 parents of children aged 5-18 in state education in England on behalf of defenddigitalme between 17th-20th February. http://survation.com/1-in-4-parents-dont-know-child-signed-systems-using-personal-data/

2 BBC Newsnight sent identifying and highly sensitive personal data http://defenddigitalme.com/wp-content/uploads/2017/06/BBCNewsnight.pdf others include The Times, Sunday Times and The Telegraph all given identifying pupil data without small number suppression

3 DfE external data shares https://www.gov.uk/government/publications/dfe-external-data-shares

4 Claim by Mime Consulting given out identifying and sensitive data http://defenddigitalme.com/wp-content/uploads/2017/06/Mime_Consulting.pdf