July 1, 2019 v.1.2

Online Harms consultation

Written submission from defenddigitalme

defenddigitalme is a non-profit, privacy and digital rights group led by parents and teachers. We aim to make all children's data safe, fair, and transparent across the education sector in England, and beyond. Our work is funded through an annual grant from the Joseph Rowntree Reform Trust Ltd. For more information please see: http://defenddigitalme.com/

1. Recommendations

1.1 Consistency of definitions and terminology
Language across government policy and legislation needs addressed if we are to avoid ever increasing scope creep or permissible interventions under unclear Codes of Practice, statutory guidance, and secondary legislation. These can come into effect with significant consequence but with little external or parliamentary scrutiny. Examples include 'threat', 'risk', and 'harm' that appear used too often interchangeably without due care or definition.

1.2 Assessment of current mechanisms
The existing availability, adequacy and effectiveness of enforcement mechanisms for handling cases of violations or abuses of the rights of the child in the digital environment should be assessed for what works or does not, before new mechanisms are introduced.

1.3 Schedule windows of opportunity to review with stakeholders
New legislation should include a planned method and timing for a review of the legislation and any subsequent Codes of Practice to evaluate their effects and effectiveness. Windows of opportunity to review should be timetabled during a transition period, and amendments possible where necessary with due consultation. Relevant stakeholders should continue to include civil society and human rights organisations, and young people themselves.

1.4 Incorporate the Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment.

1. 5 Avoid embedding existing policy harms designed into the 'online harms' space
Evidence of harm from generalised online monitoring in schools exists, and includes the chilling effect on freedom of speech, labelling individuals with longitudinal profiles, invasion of privacy in the home and family life, intrusion into confidential online communications such as children's mental health and abuse counselling support services, data collection without foreseeable consequences, foreign transfer and its distribution to an indefinite number of undetermined persons, and children gaming the systems to harm others. Unintended consequences in practice can make law unworkable and ineffective, such as on sexting. New legislation must avoid new harms, and could attempt to fix harms that have been created as a result of poor law, policy, and practice in schools and educational establishments. We welcome comments that there will be no obligation to generally monitor content, however it should go further and create safeguards on current practices.

1.6 Redress must be accessible and workable
The White Paper conflates the approach to improve reporting mechanisms to improve individual user experience, with reporting of regulatory failure at institutional level. Separating these would improve the clarity of who '*the duty of care*' is intended to deliver what support to, and at which layer of the Internet 'stack', action is intended to intervene. For users, reporting mechanisms must be tailored to be accessible to exercise the rights of a child. Regulatory oversight support must also support those who, in a qualified capacity as under Article 80(2) of the General Data Protection regulation, can champion children where they may not be aware of infringements, or have the capacity to exercise their rights.

1.7 Independence and integrity of the regulator and their role
If any external support infrastructure is to be sustainable, it must be done with transparency and avoid conflict-of-interest to demonstrate its legitimacy and retain broad trust. The oversight mechanisms for Codes of Practice should not sit under the political umbrella of the Home Office, but require broader debate and acceptance to have legitimacy, with the ability to amend or reject, which could be obtained via Parliamentary oversight.

1.8 Privacy and the reach of the obligations to be imposed by a regulator
We welcome that the paper (4.7)[1] recognises the importance of privacy and hope that the same recognition will be carried over into any legislation. The consultation section 4: *Companies in scope of the regulatory framework* on page 49 states that, "*we are consulting on definitions of private communications, and what measures should apply to these services."* We recommend that such consultation should be in the public domain. The services in scope are offered by a very wide range of companies of all sizes, including social media platforms, file hosting sites, public discussion forums, messaging services and search engines, and therefore include children's trusted confidential counselling services online. While the paper says, "*Any requirements to scan or monitor content for tightly defined categories of illegal content will not apply to private channels,*" we recommend above and beyond the no *obligation* for general monitoring (para 3.12) that an active *ban* is introduced on the general monitoring of communications of children online in particular for counselling services as defined under the scope of Article 8 under the General Data Protection Regulation, (ISS in Article 1(1)(b) of Directive (EU) 2015/1535) and categories of relevant personal data, defined as special category data, Article 9.

2. Context considerations

2.1 The UN Committee on the Rights of the Child is currently drafting a General Comment on children's rights in relation to the digital environment. We would welcome that this be taken into account during the development of legislation.

2.2 Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, *adopted by the Committee of Ministers on 4 July 2018 at the 1321st meeting of the Ministers' Deputies,* reaffirms the commitment of member States to ensure that every child enjoys the full range of human rights enshrined in the United Nations Convention on the Rights of the Child (UNCRC), in the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5), and their protocols, and that these rights should be fully respected, protected and fulfilled, as technology continues to develop.

[1] Online Harms White Paper (para 4.7, page 50) ISBN 978-1-5286-1080-3 (April 2019)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

2.3 We also suggest that evidence from the Children and the Internet enquiry (2016) is considered which includes the view on the role of government in online harms regards children with necessity and proportionately, not at the expense of paying attention offline:

> *"Lord Sherbourne of Didsbury: Can I ask about the role of Government? As I understand it, Government produced some proposals at the end of last year requiring schools to put in measures to protect children from harm online, if I am correct, and there are some proposals in the Digital Economy Bill. What further things do you think the Government should be thinking of doing? What would you like to see them doing?*
>
> *Mark Donkersley: A number of different things at different levels. It is our evidence and experience that **nearly a third of all serious behaviours we escalate are the result of offline activity—nowhere near the internet, no online activity at all.** There is very little, if any, mention of offline behaviour and how you should be trying to interpret and monitor that in any of the guidance being put forward by Her Majesty's Government. That is an issue. Nearly a third is a big hole."*[2]

2.4 This 'big hole' is not the only one. Policy makers should consider whether the emphasis on the effects of online activity on mental health in the paper is proportionate based on scant evidence, while the known need for an offline duty-of-care towards children goes unmet, evidenced across the NHS and schools. Lack of provision of qualified care is at crisis point.[3] The human support services for children in other public sectors (education, housing, libraries, SureStart, transport, universal credit et al.) have been cut, and as many councils face insolvency in 2019, we are yet to see the full extent of the harmful effects on children:

> *"This trend has been exacerbated by 'austerity' and cuts to youth services,which have been especially hard hit."* [4] (APPG onYouth Affairs Youth Work Inquiry)

2.5 Use of technology in the public sector or parenting, should not be viewed as an uncosted and commercial replacement for human support or supervision, especially for children, as there are digital side effects. As set out in the Children's Commissioner Report (2018) *Who Knows What About Me:*

> *"a clear implication of there being more public-private partnerships when delivering services to children is that more data about children is shared —often very sensitive data concerning their health or educational performance; and often without parents and children being fully aware. As Livingstone argues, it is more difficult to determine whether children's privacy and identity rights are protected in this context as there are*

[2] Children and the Internet, Lords Committee (2016) evidence from Mark Donkersley, CEO, eSafe children's monitoring software provider http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/oral/41158.html

[3] Lack of NHS mental health services puts under-18s at risk, say GPs. (December 2018) Survey shows young people struggle to access treatment and face long delays https://www.theguardian.com/society/2018/dec/30/inadequate-nhs-services-put-under-18s-with-mental-health-issues-at-risk

[4] APPG onYouth Affairs Youth Work Inquiry, Recommendations and Summary (October 2018) https://nya.org.uk/wp-content/uploads/2018/10/APPG-Summary-and-Recommendations-FINAL.pdf

> *a greater number of actors involved and the relationships between children and families and those using the data less direct."*

2.6 Further technology solutions, should take care not to seek solutionism as a goal, rather than effective tools that work, and can be demonstrated that and how they work, such as AV.

2.7 For example the current ICO proposals for Age Verification as set out in the proposed Age Appropriate Design Code of Practice give insufficient attention to the risks and benefits for children, which the ICO itself addressed in its 2016 submission to the House of Lords Consultation on Children and the Internet[5] and we included in our submission to the AACOP consultation[6]:

> ***"****there is quite a lot in the ICO evidence that you submitted to us, Mr Wood [ICO], where you stress that age verification, for example, is not an altogether useful tool, that it has drawbacks, and that anyway, as you put it, a resourceful child can almost invariably get round it."*[7]

2.8 By contrast to the enthusiasm for age verification, there is little practical discussion of the harms that derive from such policies misapplied, such as loss of privacy and its associated risks, including the risk of online fraud which is recognized[8] as the most prevalent acquisitive crime in Europe. 80% cases of identity theft use online data yet fraud and consumer protection is given little space in the consultation.

2.9 Some of the companies' promoted in the White Paper case studies are exploitative or excessive regards processing children's data, and include practices that will potentially be outlawed by the ICO Age Appropriate Design Code.

3. Need for a rights based approach

3.1 UK Ministers championed the incorporation of a rights-based approach on International Children's Day 2018, calling[9] for the UNCRC to be considered in all UK policy making:

> *"In 2010, the UK Government made a commitment to give due consideration to the UNCRC when making policy and legislation [...] I would like to reaffirm the value that this Government places on the UNCRC and our ongoing commitment to give due consideration to the UNCRC when making policy and legislation."*

3. 2 Under international human rights law there are three types of obligation on States: to respect, to protect, and to fulfil human rights. For the purpose of this text we use the same terms as the Recommendation CM/Rec(2018)7 of the Committee of Ministers to member

[5] Children and The Internet Lords enquiry (October 2016) source accessed July 1, 2019: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/oral/41158.html (https://defenddigitalme.com/wp-content/uploads/2019/06/house-of-lords-children-and-the-internet-ico-response-20160901.pdf)

[6] defenddigitalme response to the Age AppropriateCode of Practice consultation (stage two) (June 2019) https://defenddigitalme.com/wp-content/uploads/2019/06/ICO-AACOP-Consultation-defenddigitalme-v2.1.pdf

[7] Ibid Q46

[8] Williams, M. Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level *The British Journal of Criminology*, Volume 56, Issue 1, January 2016, accessed July 1, 2019 https://academic.oup.com/bjc/article/56/1/21/2462277#41881812

[9] Lord Agnew and Nadhim Zahawi, Parliamentary Under Secretary of State for Children and Families (November 20, 2018) statements HLWS1064 and HCWS1093 https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Lords/2018-11-20/HLWS1064/

States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, "child" refers to any person under the age of 18 years; and "online" or "digital environment" is understood as encompassing information and communication technologies (ICTs), including the internet, mobile and associated technologies and devices, as well as digital networks, databases, content and services.

3.3 Any systemic approach to a regulatory regime where designed to champion children's rights, must be underpinned by the overarching principles of the UNCRC which are important in the digital environment and include: non-discrimination; the best interests of the child; the right to life, survival and development; and the child's right to be heard in matters which affect them. In sum, the right to the development of a full human being free from prejudice and discrimination into aulthood, and with the promotion of their rights to human flourishing. This human rights based approach would allow scope for the enforcement of regulation on future matters outside current obvious 'harm', such as the harm from loss of autonomy, and the imbalance of power of online nudge.[10]

3.4 In contrast, the duty of care approach as described, is likely to result in an ineffective whack-a-mole type regime, managing moving targets of risk and complaint, rather than a systemic, strategic approach to supporting users in the exercise of their full rights and freedoms online.

3.5 Transparency: As set out in the UN Guiding Principles on Business and Human Rights[11] (2011)

> *"Providing transparency about the mechanism's performance to wider stakeholders, through statistics, case studies or more detailed information about the handling of certain cases, can be important to demonstrate its legitimacy and retain broad trust.*"

3. 6 That legitimacy and trust must be accountable regardless of political affiliations. Measures which define the framing of content as *acceptable* or not (8.14), based on *values* rather than *law*, put this legitimacy in jeopardy. Where content is lawful but deemed unacceptable and restricted, content censorship and perceived censorship will be the unavoidable outcome. The 2009 censorship plan 'Green Dam' planned by the government of China demonstrates how this can come about in the name of protecting children, but which fails to protect their rights and freedoms to participation, to information, access to content such as parody and political criticism, and ultimately fails to achieve public legitimacy.

3.7 Regardless of the final form of the legislation, we would also welcome if it would incorporate the Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the full rights of the child in the digital environment,

[10] BCG Henderson The Persuasive Power of the Digital Nudge (2017) https://www.bcg.com/en-gb/publications/2017/people-organization-operations-persuasive-power-digital-nudge.aspx

[11] UN Guiding Principles on Business and Human Rights (2011) https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

> *“Review their legislation, policies and practice to ensure that they are in line with the recommendations, principles and further guidance set out in the appendix of this recommendation, promote their implementation in all relevant areas and* ***evaluate the effectiveness of the measures taken at regular intervals, with the participation of relevant stakeholders;”*** [12]

3. 8 As set out in the same Recommendation CM/Rec(2018)7, the state’s mechanisms for remedy and redress should also have their own tools for assessment of their effectiveness:

> *“where appropriate, also provide children and/or their parents or legal representatives with non-judicial mechanisms, administrative or other means to seek remedy, such as through ombudspersons for children and other national human rights institutions and data-protection authorities. The availability, adequacy and effectiveness of these mechanisms for handling cases of violations or abuses of the rights of the child in the digital environment should* ***be reviewed on a regular basis.****”*

4. Realistic channels of remedy and redress

4. 1 The UN General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children’s rights[13], highlights the challenges for children to obtain remedy to problems online.

> *“There are particular difficulties in obtaining remedy for abuses that occur in the context of businesses’ global operations.” (para 67)*
>
> *“States that do not already have provision for collective complaints, such as class actions and public interest litigation, should introduce these as a means of increasing accessibility to the courts for large numbers of children similarly affected by business actions. States may have to provide special assistance to children who face obstacles to accessing justice, for example, because of language or disability or because they are very young.” (para 68)*

4.2 Regulatory mechanisms for ensuring the right to remedies and reparations for online activity are often data connected, but the government chose in 2018 to deny children a channel for this support, in the form of GDPR Article 80(2).

> *“Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78*

[12] Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment *(Adopted by the Committee of Ministers on 4 July 2018 at the 1321st meeting of the Ministers' Deputies)*
(para 1) https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808b79f7

[13] The UN General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children’s rights https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf

> *and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing."*

4.3 While data enforcement sits under the remit of the Information Commissioner, any new body with powers relevant to children may play a supporting role in fulfilling this function and any new regulatory body's powers to assess and impose sanctions on businesses which infringe children's rights should ensure it is adequately trained in the support of children and young people to fulfil this duty.

4.4 We welcome that the paper (3) recognises, '*the importance of an independent review mechanism to ensure that users have confidence that their concerns are being treated fairly.*'

4.5 We suggest that the consultation on allowing designated bodies to make 'super complaints' to defend the needs of users should be open for wide support, in particular with regard where the 'users' may be children and young people. It must be broad and not solely focussed on 'child protection' issues.

5. Issues under the current child surveillance infrastructure in schools

5.1 Infringements should not be sanctioned by state policy and our greatest concern in the White Paper is that the list of harms run close to that of those monitored under schools safeguarding software, and that the state seeks to embed unlawful practice, in new law.

5.2 The inclusion of '*Terrorist content and activity*' under harms with a clear definition, is surprising because it has no clear definition in schools' approaches conflated with radicalisation and extremism. Harms with a less clear definition also sit alongside this, in 'Extremist content and activity.' '*and activity,*' is a vague catch-all term and likely to be a net with ever-expanding scope creep.

5.3 This scope creep has created detrimental effects on children's rights in education since 2015 and tied into the use of technology for its monitoring. The consultation para 8.1 says;

> *"Technology can play a crucial role in keeping users safe online. By designing safer and more secure online products and services, the tech sector can equip all companies and users with better tools to tackle online harms. We want the UK to be a world-leader in the development of online safety technology and to ensure companies of all sizes have access to, and adopt, innovative solutions to improve the safety of their users."*

5.4 We therefore draw attention to the issues created by technology in this space, and call for them to be addressed after public consultation, or review under the Prevent programme, leading to the development of a Code of Practice for any monitoring, under this legislation.

5.5 Between 2015 and 2018 a noticeable scope creep has shifted in the Internet related schools' technology recommendations, from *filtering and blocking access* to unsuitable content, towards the proactive *monitoring* of searches and content, which includes the creation of content and communications, to now profiling and making inferences from children's behaviours.

5.6 Department for Education Statutory Guidance is issued by law; organisations must follow it unless there's a good reason not to. The 2018 Statutory Guidance, *Keeping Children Safe in Education (KCSiE)*,[14] says:

> *"The Prevent duty should be seen as part of schools' and colleges' wider safeguarding obligations. Designated safeguarding leads and other senior leaders should familiarise themselves with the revised Prevent duty guidance: for England and Wales, especially paras 57-76 which are specifically concerned with schools (and also covers childcare)."* [15]

5.7 Schools have had increasingly broad and detailed responsibilities set out since 2015 statutory guidance regarding terrorism, extremisim and radicalisation under the revised Prevent duty. Schools (and registered childcare providers) in England and Wales have been required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering."*

> *"Schools should be safe spaces in which children and young people can understand and discuss sensitive topics, including terrorism and the extremist ideas that are part of terrorist ideology, and learn how to challenge these ideas. [...] These duties are imposed on maintained schools by sections 406 and 407 of the Education Act 1996. Similar duties are placed on the proprietors of independent schools, including academies (but not 16-19 academies) by the Independent School Standards."*[16]

5.8 The drift in ***what*** is considered significant activity, has been from terrorism into now more vague and broad terms of extremism and radicalisation, from some assessment of *intent* and *capability of action*, towards interventions for potentially insignificant potential vulnerabilities and *inferred assumptions of disposition* towards such ideas. A similar sense of shift was also identified as an issue in the programme more widely by academic Dr Therese O'Toole in the Citizenship and Civic Engagement Committee report, *The Ties That Bind*:[17]

5.9 As RightsWatch UK set out in their 2016 report, Preventing Education[18],

> "*The definition of extremism is meaningfully different from the definition of terrorism set out in section 1 of the 2000 Act. Terrorism, according to the 2000 Act, entails the 'use or threat of action ... designed to influence the government ... or to intimidate the public or a section of the public' 'for the purpose of advancing a political, religious or ideological cause.'52 Further, the 'action,' must be of a kind which 'involves serious violence against a person, involves serious damage to property ... endangers a person's life, other than that of the person committing the action, ... creates a serious risk to the health or safety of the public or a section of the public, or ... is designed seriously to interfere with or seriously to disrupt an electronic system.' The Court of*

[14] Ibid p83

[15] September 2018 DfE Guidance Keeping Children Safe in Education https://defenddigitalme.com/wp-content/uploads/2018/12/Keeping_Children_Safe_in_Education__3_September_2018_14.09.18.pdf

[16] Revised Prevent Duty Guidance: for England and Wales (2015) page 7 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

[17] Citizenship and Civic Engagement Committee (April 2018) The Ties That Bind report on Citizenship and Civic Engagement https://defenddigitalme.com/wp-content/uploads/2019/03/The-Ties-that-Bind-Prevent-Report-April-2018-.pdf

[18] Preventing Education? Human Rights and UK Counter Terrorism Policy in Schools, RightsWatch UK (2016) report http://rwuk.org/wp-content/uploads/2016/07/preventing-education-final-to-print-3.compressed-1.pdf

> *Appeal has recently confirmed that, for an action to constitute an act of terrorism, the perpetrator must intend that the action will have one of those outcomes (violence, risk of harm, etc) or be reckless as to such an outcome.*"

6. Section 8: Technology as part of the solution

6.1 The paper section 8. suggests that the government and the new regulator will work with leading industry bodies and other regulators to support innovation and growth in this area and encourage the adoption of safety technologies.

6.2 We would welcome if government will also work more closely with a diverse range of industry and civil society expertise to develop a safety-by-design framework for monitoring, linking up with existing legal obligations around data protection by design and secure by design principles, and privacy preserving solutions.

6.3 On Filtering and Monitoring explicitly, the new DfE 2018 guidance (Annex C) says;

> *"Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place.*
>
> *"Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks. The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty."*

6.4 Ofsted 2018 guidance on *Inspecting Safeguarding in Early Years, Education and Skills Settings*[19] suggests settings must have more specifically, "*appropriate filters and monitoring systems are in place to protect learners from potentially harmful online material.*" (Age 2-5)

6.5 The DfE Annex C on the Prevent duty, signposts readers to the UK Safer Internet Centre [20] which, has guidance on what "appropriate" filtering and monitoring might look like:

> *"UK Safer Internet Centre: appropriate filtering and monitoring. Guidance on e-security is available from the National Education Network. Support for schools is available via the: schools' buying strategy with specific advice on procurement here: buying for schools.Whilst filtering and monitoring is an important part of the online safety picture for schools and colleges to consider, it is only one part."*

6.6 Between 2015 and 2018 there was no guidance on whether or not personal devices should be monitored. In 2018 this changed, but only with reference to over-blocking, ie not to overly restrict access to content, so the guidance's sense of proportion is lost in practice.

[19] Ofsted: Inspecting safeguarding in early years, education and skills settings (October 2018) (p13) https://defenddigitalme.com/wp-content/uploads/2019/03/Inspecting_safeguarding_guidance_061118.pdf

[20] UK Safer Internet Centre fails to make any mention of the lawful basis for such monitoring nor its limitations for example of personal devices and personal devices, spaces, and time.

6.7 There are no public metrics on the volume of blocking in schools, and its success rates or otherwise, despite the significant costs this incurs for schools. Any company operating such services should publish an agreed mandatory set of transparency statistics.

6.8 Given that web blocking is on the increase globally, with precedents in law set in Turkey, and Russia and Azerbaijan on internet regulation, including new powers for the Government and domestic courts to block websites,[21] we must take extreme care over the effect of our international outward facing actions. The Foreign Office work in freedom of the press[22] would be wasted and entirely at odds with restrictive Internet regulation that is or were to appear to be politically controlled.

6.9 On the invasion of privacy and policy at home, there is no Code what the Statutory Guidance (Annex C) from the Department means, and there is a clear breach of privacy and the right to family life, where it regards personal devices and home monitoring. The Court of Justice of the European Union in X v Commission [1994] ECR I-4347 has said (para 17) that the right to respect for private life, embodied in article 8, "*includes in particular a person's right to keep his state of health secret*". Schools are unable to maintain this guarantee the security of a person's data against unauthorised access, when the functionality of web monitoring is outsourced to third party companies, made available to an unknown and indefinite number of persons, and may in some cases, be transmitted outside the UK and EU. These monitoring activities need enforcement correction, and oversight.

> *"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. ...When you look at the school holidays just gone, we were probably averaging something like 200 serious incidents a week. A high proportion of those were illegal, life-threatening, and therefore, again, we are filling a gap that a school would find very difficult to meet regarding attempting to monitor behaviour, and what has happened there is the devices have travelled home with the student or the staff member—because we are monitoring staff as well."*

7. The ethics and education of online harms in schools

7.1 The limits of school reach are no longer school premises, but the '*home with the student or the staff member'*. This encroaches on privacy, in law as well as ethics beyond the questions of how to regulate content, and what the role of technology is to do so.

7.2 Much of this online monitoring is done through algorithms that match search terms and sites against libraries of keywords. The High Level Expert Group on Artificial Intelligence recently recommended in their report on the Policy and Investment recommendations for Trustworthy AI, that (4.1):

[21] European Human Rights Advocacy Centre, Middlesex University, (June 2017) http://ehrac.org.uk/news/critical-websites-challenge-block-azerbaijan/

[22] Foreign Secretary sets out his vision to improve media freedom around the world (May 2, 2019) https://www.gov.uk/government/speeches/foreign-secretary-sets-out-his-vision-to-improve-media-freedom-around-the-world

> "*Children should be ensured a free unmonitored space of development and upon moving into adulthood should be provided with a "clean slate" of any public or private storage of data related to them.*" [23]

7.3 We have been told of children wrongly labelled through proactive monitoring software, and the lack of schools ability or willingness to delete data inferred by mistake, for fear of future reprisals.

7.4 Providers and some IT technicians in schools argue that this is the flaw of the policy and practice, not systems. Some practice includes monitoring by photograph taken via web cam.

7.5 However the very existence of *secret* keyword libraries which may create inferences and profiles upon matching with words used by the child, is opaque by design, and without foreseeable consequences. Systems must be designed so that children can access their rights not deliberately make them impossible or hard to understand by design.

7.6 Neither children nor families understand how this processing works to the degree required under Data Protection law. While UKCCIS guidance[24], says it is a basic requirement in privacy and security training for children in schools to understand how monitoring works, our research and a poll in February 2018 shows it does not happen. Over 86% of 1,004 parents and guardians asked by Survation in a 2018 poll,[25] agreed that they should be informed how monitoring and keyword logging works, and its consequences. Similar numbers believed that children needed to be informed what these words are.

7.7 Companies decline Subject Access Requests about online harms profiles, and refer pupils / parents back to schools, which does not provide a picture of the data processed by the company or profiles that they hold from Internet searches or keyword library matching. The Online Harms legislation should support a child's right to transparency and autonomy.

7.8 Children want to understand how their data are processed and restore fairness in systems, and 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).

8. Rights respecting technology by design and regulation of use

8.1 The *UN General comment No. 16 (2013) on State Obligations regarding the impact of the Business Sector on Children's Rights*[26], further requires the obligation on the public sector in its procurement and promotion of technology, to respect children's rights and not support companies that promote violations:

[23] Policy and Investment Recommendations for Trustworthy Artificial Intelligence (accessed July 1, 2019) (published June 26, 2019) https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence (permanent copy https://defenddigitalme.com/wp-content/uploads/2019/07/AIHLEGPolicyandInvestmentRecommendationspdf.pdf)

[24] UKCCIS guidance Education for a Connected World (p37) https://defenddigitalme.com/wp-content/uploads/2019/03/Education_for_a_connected_world_PDF.pdf

[25] Survation poll of parents of children aged 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

[26] The UN General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf

> *"to respect also implies that a State should not engage in, support or condone abuses of children's rights when it has a business role itself or conducts business with private enterprises. For example, States must take steps to ensure that public procurement contracts are awarded to bidders that are committed to respecting children's rights. State agencies and institutions, including security forces, should not collaborate with or condone the infringement of the rights of the child by third parties. Furthermore, States should not invest public finances and other resources in business activities that violate children's rights."*

8.2 We agree with the statement in the white paper (2.12) "*Many companies claim to hold a strong track record on online safety but there is limited transparency about how they implement or enforce their policies*" and we would welcome measures to change this. Both children's and staff personal data are currently under general monitoring in schools.The underpinning design principle of these technologies is to breach privacy and data protection by design, not to protect it as required under GDPR Article 25.

8.3 Some systems even override the school supervision and human-in-the-loop, with one school IT technician saying they disagree with the eSafe approach that the company, "*monitor externally and will call the police if they detect something extremely serious, even if the school doesn't consent to this."*

8.4 Evidence from 4,507 of 6,950 schools that carried out e-safety self-reviews, using the 360 Degree Safe SWGFL tool in analysis carried out by Professor Andy Phippen[27], shows school staff are not equipped to deal with or challenge the outcomes from these technology. Behavioural effects are under researched, but their qualitative feedback suggests a chilling effect on searches for sexuality, health, and teenage development questions.

8.5 Fifty per cent (50%) of 400 schools that have responded to us via FOI impose on Bring-your-own-device which is opaque level of surveillance of personal property, active wherever logged in to school network and some at all times regardless of network.

8.6 In Barbulescu vs Romania, the court found that an employer's instructions could not reduce private life in the workplace to zero. There is also a right to reasonable expectations, to access personal data created, to rectification, to be able to contest any conclusions drawn from the data processing, and appropriate right to redress. This should similarly apply to students as well as school staff.

8.7 There is no mechanism for identifying technical flaws, bias, racism or discrimination built in by design and it is likely that some languages are targetted more than others. CEO of e-Safe for example told the Lords select committee in 2016 that,

> *"Often, the more serious behaviours, again, are being articulated in a foreign language, maybe Urdu script or Arabic script."*

8.8 And there is no oversight of consistency of what is escalated, depending on which keyword matches, which system, and can be based on little more than opinion and 'belief':

[27] Invisibly Blighted, The digital erosion of childhood, Leaton Gray, S. and Phippen, A. (p56) Sage publications (2017) ISBN: 9781782770503

> *"That technology is effectively watching the material coming to the device screen—so your laptop, what images are appearing there, whether they are moving or static; ...It is watching the words and phrases coming to the screen, it is looking at the keystrokes entered into the device, and it is looking at material and activity conducted from connecting devices, so pen drives, downloads from mobile phones, that sort of thing. When the technology detects material it feels is inappropriate or it matches what we call our threat libraries—these are literally tens of thousands of terms, phrases, euphemisms, slang, in multiple languages associated with a range of behaviours, whether it be paedophile grooming, child abuse, FGM, bullying, self-harm risk and so on and so forth—if something triggers, we receive a screenshot of what the user was looking at on the screen at that moment. That screenshot is reviewed by a team of multilingual behaviour specialists, as I say, based in Salford, and they will review that incident in context and, depending on what they believe is going on, they will escalate that incident if necessary…"*

8.9 The consequences of such profiling and systems' use are so significant that it is reckless to engage them without qualified use. Lack of capability and training, does not absolve staff of accountability for the data management responsibilities that occur under their control.

9. Recommendations for change on managing online harms in schools

9.1 Clarity, consistency, and consultation

The Department for Education should develop and issue comprehensive guidance what constitutes "appropriate" filtering and monitoring, in order to ensure that schools and colleges adopt and implement policies and processes that are lawful, consistent and proportionate. Guidance should assist schools to comply with the Data Protection Act 2018, human rights law, and other standard requirements and be developed through a public consultation process.

9.2 Statutory Code of Practice on filtering and monitoring

The Department for Education, the Information Commissioner's Office, and Ofsted should support the development of a statutory Code of Practice on filtering and monitoring to which schools and colleges must adhere. The Code should include a due diligence requirement, and create a non-exhaustive set of safeguards which schools must put in place before allowing any third-party company or body access to children's personal data, and consistent rules on retention, errors, and redress. Compliance in the everyday practice should be enforced through existing Ofsted audit and inspection, and could be developed under the Online Harms framework, under the oversight of the national online harms Regulator.

9.3 Transparency duty

Commercial companies providing monitoring services should be regulated and required to transparently report. This may include considerations such as filtering rates and content, blocking and monitoring capability expansion, profile categories, data retention, access and distribution, logfile volumes and content, correction rates and redress. At school level, a report should be provided to parents and pupils on an annual basis, made available on request, and be regularly reviewed to ensure practice complies with the principles of necessity and proportionality.

9.4 Informed fair processing and improving digital literacy

To ensure children and young people are informed about their data processing, schools and colleges should provide pupils, parents and staff with adequate information, tailored for different age groups, to understand how their online activity is monitored and recorded, and that and how they can be tracked, profiled and reported to third-party agencies and bodies. Before being asked to opt-in to Home-School IT agreements, pupils and parents must be informed how monitoring and keyword logging works and its consequences, and of any web camera surveillance. Requirements would be set out in a Statutory Code of Practice (2).

9.5 Fairness and transparency for children and families

Monitoring systems must enable schools to provide a consistent report to children and families as easily as they already report profiles and log file information to the Designated Safeguarding Lead. Who knows what about me should be an easy question for a child to ask a school to fulfil and schools should have a duty to provide this information on an annual basis, or on demand.

9.6 Staff training obligations

School staff should receive mandatory instruction on data protection and privacy by design as part of online safety training. This should include clear explanations of all student and staff monitoring systems functionality and reporting mechanisms.

9.7 Oversight

The Children's Commissioner believes that, "we are failing in our fundamental responsibility as adults to give children the tools to be agents of their own lives." Her recommendation for a children's Digital Ombudsman could be met, in part, by this regulator. Targeted home web monitoring of children for the purposes of the Prevent programme, should further require judicial oversight.

10. White Paper Box 33: Google Family Link

10.1 We note the inclusion of Google Family Link in Box 33. Google's Family Link app allows parents to view and control apps and even remotely lock a [child's] device.

10.2 However government should consider whether it is appropriate to be seen to promote a commercial company app which sends advertising to children or personalised content, as a result of their use. The Family Link approach to serving ads to children, seems out of step with the 'best interests of the child' approach in parallel measures by the ICO Age Appropriate Design code.

> *"Google will not serve personalized ads to your child, but your child will still see ads while using Google's services."* [28] *"We collect information about your child's activity in our services, which we use to do things like recommend apps they might like on Google Play."*[29]

[28] Family Link Disclosure for Parents of Children under 13 (or applicable age in your country) https://families.google.com/familylink/privacy/notice/

[29] Family Link Disclosure for Parents of Children under 13 (or applicable age in your country) Privacy policy https://families.google.com/familylink/privacy/child-policy/

10.3 Furthermore, the app has what appears to be an extensive and excessive data collection and retention from the child:

> *"We collect information about your child's activity in our services, which we use to do things like recommend apps they might like on Google Play. Your child's activity information that we collect may include things like search terms, videos they watch, voice and audio information when they use audio features, people with whom they communicate or share content, and Chrome browsing history they've synced with their Google Account. If your child uses our services to make and receive calls or send and receive messages, for example by using Google Hangouts, we may collect telephony log information like their phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls.*
>
> *"We may collect your child's voice and audio information. For example, if your child uses audio activation commands (e.g., "OK, Google" or touching the microphone icon), a recording of the following speech/audio, plus a few seconds before, will be stored to their account from any of your child's signed-in devices, when the Voice & Audio Activity setting is enabled.*
>
> *"In addition, we may combine the information we collect among our services and across your child's devices for the purposes described above. Depending on your child's account settings, their activity on other sites and apps may be associated with their personal information in order to improve Google's services."*

10.4 DCMS should also ask Google why its minimum age requirements "*may not be applicable to G Suite users, including accounts in G Suite for Education domains*," [30] in the UK, noting that consent is not a lawful basis available to the public sector for everyday processing.[31]

10.5 The further privacy risk from this app, comes from setting up children to be automatically notified that they can now choose to be removed from parental oversight of Family Link on their thirteenth birthday, and then from 18, are served up to the full Google advertising machine of AdSense: 18+ and Google Ads: 18+[32].

10.6 Rather than protecting children, certainly from any harms to privacy, Family Link could be seen as a neat way of legitimately working around rights under the umbrella of data protection law, and monetising children with the impunity of 'consent' from the very first day of adulthood.

[30] Family Link Disclosure for Parents of Children under 13 (or applicable age in your country) https://support.google.com/accounts/answer/1350409

[31] When is consent appropriate? (ICO) Accessed July 1, 2019 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/

[32] Family Link Disclosure for Parents of Children under 13 (or applicable age in your country) https://support.google.com/accounts/answer/1350409

11. Online harms in scope

11. 1 Screen Time

Underage exposure to legal content includes the harm, excessive screen time. We point out that whilst popular opinion and media concerns mount over how *screen time* and social media affect children, Professor Dame Sally Davies, England's chief medical officer, found no such evidence in a review.[33]

> *“Scientists examining child development and technology use have for years been trying to raise awareness of the misguided debate around children and screen time; a debate often devoid of significant scientific evidence. The common comparison between screen time and drugs like alcohol indicates a misconception many politicians and journalists share. Screen time isn’t a chemical that, when ingested, causes concrete physiological changes that can harm the body and cause long-term dependency. It is a diverse and ever-changing part of daily life. First, there is no concrete evidence that supports the common view that technology use is inherently harmful.”* [34]

11.2 Sexting

Inclusion of sexting among a ‘harm’ with a clear definition, should be disputed.

> ‘*Sexting of indecent images by under 18s (creating, possessing, copying or distributing indecent or sexual images of children and young people under the age of 18).’*

We have been told by police, school liaison and school staff that this is routinely ignored, so as to encourage young people and children to speak openly and trust interactions with school staff and police. Criminalisation of teenagers because of intimate photos on their phones, especially where no malicious intent exists, deters trust and openness and causes harm in itself.

The legislation should seek to end this harm, as a result of poor law, not further embed it.

We are happy to answer any questions on request, and to be contacted for further consultation on request.

Defenddigitalme
July 1, 2019

[33] Chief Medical Officer (February 2019) commentary on ‘Screen-based activities and children and young people’s mental health and psychosocial wellbeing: a systematic map of reviews’ https://defenddigitalme.com/wp-content/uploads/2019/07/UK_CMO_commentary_on_screentime_and_social_media_map_of_reviews.pdf

[34] Why Hunt's screen time limits for kids are scientific nonsense. (Orben, A.) Guardian April 2018 https://www.theguardian.com/science/head-quarters/2018/apr/23/why-hunts-screen-time-limits-for-kids-are-scientific-nonsense