Keeping Children Safe in Education - Department for Education Consultation Response

Draft: Statutory Guidance September 2016' [1]

We would like to draw attention to three areas of focus with respect to Paragraph 75, p22:

"Governing bodies and proprietors should be confident that systems are in place that will identify children accessing or trying to access harmful and inappropriate content online. Guidance on e-security is available from the National Education Network."

- Lack of public engagement and democratic debate
- Pupil privacy and confidentiality
- Practical considerations

We suggest that this proposal which will monitor every child in school's online activity and communications, the vast majority of whom will never need any intervention as a result, is significant and if it is to become statutory practice, should be assessed more deeply in a separate consultation and widely debated in public and Parliament.

Recently topical security-related issues appear conflated with child welfare into a poorly defined safeguarding label when in fact they require addressed differently both in their practical, and in data privacy and protection terms and application.

It is the data privacy aspects and impacts of change that we focus on in our brief submission.

Lack of public engagement and democratic debate

1. The 'who this is for' in the guidance[2] excludes the public, and any experts in data privacy, data protection and cyber security. This is unwise given the nature of the requirement in paragraph 75.

- Schools and college staff
- Governing bodies, proprietors and management committees
- Children's services
- Professionals working in social care
- Teaching Unions
- Safeguarding practitioners

2. This new guidance makes no attempt to ensure public engagement. The relationship of trust between teacher and pupil is an important one for young people growing up. The potential for risk and harm to young people as a result if this role of trusted elder is undermined should not be underestimated.

---

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/487799/Keeping_children_safe_in_education_draft_statutory_guidance.pdf

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/487735/Keeping_children_safe_in_education_consultation.pdf

3.We believe that if the intent of this guidance is to require monitoring software use of every child and young person in education in England, there should be a distinct public consultation on the principles, approach and code of practice.

4.Without any code of practice to accompany this draft guidance it is impossible to fully understand what common and consistent principles, approach and privacy assessment will be made before, and after the implementation of new monitoring practices.

5.The recommendation of the 2014 Select Committee Report "Responsible Use of Data" [3] recommended that; "*the Government has a clear responsibility to explain to the public how personal data is being used*." This should be a guiding principle in all but the minority of exceptional circumstances in all datasharing activity in, across, and outside of schools using pupil data. Data legislation requires it, and it should be upheld in both the spirit and letter of the law.

Pupil Privacy and Confidentiality

6.Firstly we also note that in practical terms Paragraph 88, p24 appears oddly phrased and needs clarification: "Governing bodies and proprietors should ensure that staff members do not agree confidentiality and always act in the best interests of the child." Confidentiality is often in the best interests of the child. The intention of this sentence is unclear but we would want to ensure that whatever was intended would be clear and how it should be applied in practice explained.

7.Common law confidentiality is both a requirement and important consideration in the nature of the relationship in schools between trusted elder and children, and their parents.

8.The rights to confidentiality and privacy are enshrined in human rights law, and more stringently for children. We ask what privacy impact assessment has been carried out given that this will be statutory guidance?

9.Has the Joint Committee on Human Rights reviewed it for the effect on privacy and intrusion into family life? They have noted previously, "failure to root human rights in the mainstream of departmental decision-making".[4]

10.Has any existing automated decision-making in schools using these software been assessed for the legal[5] and practical application they deserve? Discriminatory[6] uses of profiling data are widely recognised to exist and may be harmful in children, with unforeseen lifetime impacts and recourse difficult to get, based on system-based decisions pupils may find inaccessible or hard to challenge.

11.What requirement is there in schools for transparent publication of software partners, third party use, their privacy terms and conditions?

---

[3] http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf

[4] http://www.publications.parliament.uk/pa/jt200708/jtselect/jtrights/72/72.pdf

[5] https://www.privacycommission.be/sites/privacycommission/files/documents/convention_108_explanatory_report.pdf

[6] http://www.fipr.org/childrens_databases.pdf

12. What rights are granted to individuals to have data corrected, removed, or expunged from records and how long after the event is noted may these data be accessed and by whom?

13.Since the aim is that "systems are in place that will identify children" it is clear that identifying data are to be collected.

14.In terms of Data Protection law, there should be a clear and transparent assessment made by the Information Commissioner's Office of the types of data that are to be collected in this manner.

15.How these may be handled and treated will vary depending on their type, sensitivity and the purposes for which they are collected. This requires expert qualified data protection assessment together with expert knowledge of the Data Protection principles and their application, and with the particular considerations they require for children.

16.There should be consistent application if it is to be a nationwide statutory requirement. To leave this to schools and individual providers to apply, risks a postcode lottery in the fair application of privacy and protection rights, which may not safeguard from, but potentially expose vast numbers of children to, risk.

Questions that the consultation raises in practical application

In this area a large number of practical questions follow which the guidance makes no attempt to address. A selection for consideration include oversight, proportionality, retention, and transparency.

17.Remembering that 85% of children's waking hours are spent outside school[7], and in a wide range of schools for our children aged 2 -19, widely varying amounts of school time is spent on-screen, is it appropriate that this 24/7 monitoring would be applied to all types of school?

18.Will monitoring be applied to all bring-your-own-devices (BYOD) and home use monitored?

19.How will use on shared-computers, particularly if BYOD is in use, be justly and legally applied?

20.What due diligence is done with the providers of these software who will have direct access to the equipment and data of millions of children?

21.Are data retained by third-party providers? Research suggests that some manage the service directly, removing the school classroom staff from the process until after violations of policy are detected and report sent to the school headmaster and 'safeguarding staff'.

Consent: the importance of clear privacy notices to understand what we sign up to

22.While consent may be one condition for processing, this does not mean that by consenting to use a system in school pupils trade all their privacy rights. The collection and processing of their personal data must still be fair and lawful, and pupils and guardians retain their rights under the DPA including the requirement that consent cannot be too broad. Consent must be freely given and informed, needing special consideration for children, given their vulnerability, and particularly with

[7] http://www.publications.parliament.uk/pa/cm201012/cmselect/cmeduc/744/744i.pdf

reference to the threshold of Gillick competency. This may also require an approach to parents and ensure complete and informed consent process takes place, with alternative provision on offer.

23. What alternative is offered to parents and pupils who do not consent to this broad data collection and processing and/or use by third parties?

Conclusions

24. We do not believe that clear and specific rights or responsibilities are sufficiently outlined in this guidance to enable thorough assessment of risk and both the tangible and intangible cost of its implications. Further information is required about the principles and their practical application of the requirement outlined in paragraph 75, in transparent public and Parliamentary debate.

25. While complex with conflated issues,[8] children's safeguarding, should not a priori compromise children's basic dignity and their rights to be respected, and trusted. The UN Convention on the Rights of the Child [9] explicitly states their right to privacy, freedom from surveillance or censorship and the right to online anonymity. These must be respected in statutory guidance and practice.

We are happy to discuss any details or questions.

Jen Persson, coordinator
defenddigitalme
February 2016

About defenddigitalme

defenddigitalme's campaign asks the Department for Education (DfE) to change their policies and to protect 20 million[10] children's identifiable personal data in the National Pupil Database (NPD):

- Stop handing out identifiable personal data to commercial third parties and press
- Start telling pupils, their guardians and schools what DfE does with personal data
- Be transparent about policy and practice

We want to see legal and regulatory frameworks fit for our children's digital future and call for:

- secure handling of sensitive identifying pupil data
- statutory privacy impact assessments and public consultation
- the legislative review of DfE sharing of children's personal data
- the separation of consent for identifiable data required for school administration from secondary use commercial purposes

We are supported by a number of parents, pupils, legal, data privacy and data protection experts.

---

[8] http://eprints.lse.ac.uk/60727/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Livingstone%2C%20S_Childrens%20digital%20rights_Livingstone_Childrens%20digital%20rights_2015.pdf

[9] http://www.unicef.org/crc/files/Rights_overview.pdf

[10] http://www.fft.org.uk/FFT/media/fft/Downloads/FFT-Story.pdf