Case for a Code of Practice on Processing Personal data in Education

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.

1. The GDPR, Global and UK context for a Code of Practice

1.1 We ask you to support an amendment that would require the Information Commissioner to create and publish a statutory Code of Practice for the education sector.
[Suggested draft text is on page 4.]

1.2 **Lord Knight** at Second Reading said[1]: *"Schools routinely use commercial apps for things such as recording behaviour, profiling children, cashless payments, reporting and so on. I am an advocate of the uses of these technologies. Many have seamless integration with the school management information systems that thereby expose children's personal data to third parties based on digital contracts.* ***Schools desperately need advice on GDPR compliance to allow them to comply with this Bill when it becomes law."***

1.3 At Second Reading, **Lord Storey** said, *"young people probably need more protection than at any other time in our recent history. They should have control over their own data."*[2]

1.4 **Lord Lucas** asked practical questions that businesses need to know, "*How is age verification supposed to work? Does it involve the release of data by parents to prove that the child is the necessary age to permit the child access, and if so, what happens to that data?"*[3]

1.5 GDPR recognises the principle in **Recital 38, children** "***merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.****"*

1.6 UNICEF's recent working paper on children Privacy, Protection of Personal Information and Reputation[4] says it is evident, "***children's privacy differs both in scope and application from adults' privacy*****,"** and they "**experience more threats than any other group."** Our UK Bill as yet fails to bring in many of the safeguards the GDPR suggests, especially on profiling.

1.7 The Council of Europe 2016-21 Strategy on the Rights of the Child recognises the digital environment exposes children to *"privacy and data protection issues,"*[5] and that "*parents* ***and teachers*** *struggle to keep up with technological developments."* Note: there is no standard data protection or data privacy in basic teacher training, despite the value of edTech set out in the UK Digital Strategy.[6]

1.8 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.[7]

[1] Data Protection Bill Second Reading, 10 October 2017 Hansard, Lord Knight of Weymouth https://goo.gl/cxSZXM
[2] Ibid, Lord Storey https://goo.gl/dKaJvX
[3] Ibid, Lord Lucas, https://goo.gl/723xfc
[4] UNICEF working paper http://defenddigitalme.com/wp-content/uploads/2018/02/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf and Children and the Data Cycle: Rights and Ethics in a Big Data World https://www.unicef-irc.org/publications/pdf/IWP_2017_05.pdf
[5] Council of Europe Strategy for the Rights of the Child 2016-21 https://rm.coe.int/168066cff8 p10/26 (6) Para 21.
[6] UK Digial Strategy 2017 https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy
[7] Growing up Digital Taskforce 2017 https://www.childrenscommissioner.gov.uk/publication/growing-up-digital/

2. Recommendations for Codes of Practice for Children

2.1 **We recommend a statutory code for schools to help implement the GDPR to deliver:**

- Clarity in schools what can and cannot be done, especially on the boundaries of public and legitimate interests, and consent, and where GDPR may require changes compared with today.
- Confidence in schools in their responsibilities to handle data well when sharing with social services in direct care, for indirect use in research, or buying and using trusted edTech safely.
- Consistency and fairness in how children, parents and carers are informed of rights and about the use of personal data by third-parties, at local, regional and national levels across the UK.

2.2 **A code would enact the Working Party 29 explicit recommendation to create guidance** about children on profiling and automated decision-making with significant effects recognising that in Recital 71, such a measure '*should not concern a child.*'The WP29 noted,"Article 40(2) (g) explicitly refers to the preparation of codes of conduct incorporating safeguards for children."

2.3 **The International Working Group on Data Protection in Telecommunications** summed up in their Working Paper on e-learning platforms in April 2017:[8] "The sensitivity of digitized pupil and student data should not be underestimated. Legislation covering *educational institutions may not adequately address new technological trends in learning processes and the extended scope and purposes of data processing in the context of e-learning and learning analytics."*

2.4 **Growing up with The Internet House of Lords Report, March 2017**:
"Any future policy should be based on principles which firmly place children's rights, wellbeing and needs as the preeminent considerations at all points of the internet value chain where the end user is a child. ***This shared responsibility requires all stakeholders,*** *and commitment [...] in what is a rapidly changing landscape that will include the Internet of Things and Artificial Intelligence."* [9]

3. Children's Rights

3.1 Not only have children no choice how their personal data are used in education, it can pose real risk of harm and loss. Providers fail to make products safe such as UK school CCTV found streaming on US sites. In 2017 over 2 million UK pupil-teacher accounts were stolen from platform Edmodo.

3. 2 Our children's full development and flourishing may be supported but may also be limited by data about them; through labels given to them for life or their digital footprint compromised in school. The Council of Europe 2016-21 Strategy on the Rights of the Child,[10] has an entire section on the digital world. It makes clear that, *"Children have the right to be heard and participate in decisions affecting them"* and recognises that capacity matters, ***"in accordance***

[8]The International Working Group on Data Protection in Telecommunications (IWGDPT) was established in 1983 by a number of national data protection authorities http://defenddigitalme.com/wp-content/uploads/2018/02/25042017_en_2_elearningplatforms.pdf
[9] https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/130.pdf Paragraph 353, Growing up with The Internet, March 2017
[10] Council of Europe Strategy for the Rights of the Child 2016-21 Para 37, p15/36 https://rm.coe.int/168066cff8

with their age and maturity*"*. In particular attention should be given to *"empowering children,* ***such as children with disabilities.****"*

3.3 This code should be inclusive **for children** (up to age 18 for purposes of GDPR except where stated) **and pupils** (defined by the Education Act 1996, up to age 19) and further **individuals up to the age of 25 in education, with special educational needs and disability.**

3.4 A code should clarify how and where capacity should be considered in applying the legal basis for processing personal data from children, such as freely given consent.

3.5 The UNCRC demands policy makers aim to ensure every child is **safe**, has effective access to and receives education, services, and recreation opportunities - to develop **to their fullest potential.** Article 12 of the Convention on the Rights of the Child (the Convention) a right to be heard, addresses the legal and social status of children, [...] subjects of rights. It is vital to balance the rights of safety, privacy, and participation including the views of young people.[11]

4. Definitions for children and pupils and on age differences

4. 1 Compulsory education ages and definition of "pupil" are different across the UK, and within the meaning of the 1996 Education Act[12] (may be up to age 19); the Education (Scotland) Act 1980, The Education and Libraries (Northern Ireland) Order 1986, or young people with special educational needs or disability within the Children and Families Act 2014.

4. 2 Consistent approaches to child rights as regards data should apply across the UK and across all types of educational setting for children under 18, the de-facto "child" in GDPR.

4.3 Parental responsibilities and oversight of consent can continue up to age 25 with SEND or an EHC plan in education, but for whom the Bill makes no provision beyond age 18. While SEND legislation takes account of this; without any mention of capacity, this Bill does not. A code should give clarity for example on the edges of parental and pupil consent to SEND data processing, how terms and conditions must be explained, and take account of all young people in education, so that everyone's rights are more fairly recognised, explained and respected.

5. Why this is needed and separate from Clause 124

5. 1 The amendment added to the Bill in the House of Lords requires the Information Commissioner to publish a statutory Age-Appropriate Design Code to establish standards of design that data controllers must meet for Information Society Services (GDPR Article 8).

5. 2 It is for *online services* "likely to be accessed *by a child*" (under 18s) and will not apply to the majority of personal data collected "*about children,"*processed without consent.

5.3 After the introduction of Lady Kidron's code, peers discussed the need for better understanding in education. **The Earl of Clancarty said**, *"Both children and parents need to be properly informed of these rights and the use to which data is put at every stage throughout a child's school life and, where applicable, beyond."*[13]

[11] The Internet on our Own Terms: How children and young people deliberated about their digital rights.(2017) Coleman, S., Pothong, K., Vallejos, E.P and Koene, A. (University of Nottingham, Horizon Digital Economy Research, 5Rights)
[12] The Education Act (1996) meaning of "pupil" http://www.legislation.gov.uk/ukpga/1996/56/section/3
[13] Hansard, col 1436 December 11, 2017 The Earl of Clancarty, https://goo.gl/FbBvxk

5.4 The processing of children's personal data in education is everyday in schools, and reaches into the home[14] and private life, through school information management systems; absence and health administration apps; biometric cashless systems; teacher led[15] classroom or behaviour tracking apps; security pass systems; or termly national school census. For common case studies of children's profiling in education in England see our submission to WP29.[16] p3-5, including racial and behavioural profiling, and monitoring by school software at home.

5.5 Often data collection is required by the State through legislation. In England millions of children's identifying and sensitive data[17] are regularly distributed by the Department for Education to third parties including journalists, and named[18] data for research. Children and parents are not asked for consent. Parents have no oversight who has our child's personal data or why and has lost control of a child's digital footprint by age 5. According to analysis by defenddigitalme, over 86% of the releases since 2012 were of individual level, identifiable and sensitive or highly sensitive data.

5.6 Lord Stevenson said even about deidentified data, "we should look at this again.[...] others may want to speak to the risk that it poses also to children, in particular." [Col 210]

[14] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/oral/41158.html *"not confined to the school bell starting in the morning and [...] the afternoon, it is 24/7 and it is every day of the year."*

[15] Class Dojo poses Data protection Concerns for Parents (2017) Williamson, B. and Rutherford, A. http://blogs.lse.ac.uk/parenting4digitalfuture/2017/01/04/classdojo-poses-data-protection-concerns-for-parents/

[16] Submission on the WP29 guidance on automated processing and children - sample case studies in England pp 3-6 http://defenddigitalme.com/wp-content/uploads/2017/12/DDM_Response-to-Working-Party-29-Guidelines-on-Automated-individual-Decision-making-and-Profiling-for-purposes-of-Regulation-2016_679_v1.2-2.pdf

[17] http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-12-18/120141/

[18] http://defenddigitalme.com/2016/02/scope-creep-in-national-pupil-database-now-means-names-released/

6. Draft Code on Processing Personal Data in Education [draft]

After Clause 124

Insert the following new Clause— "Code on processing personal data in education where it concerns a child; or a pupil within the meaning of the 1996 Education Act; the Education (Scotland) Act 1980, The Education and Libraries (Northern Ireland) Order 1986, or children and young people with special educational needs or disability with the meaning of the Children and Families Act 2014 and Code of Practice.

(1) The Commissioner must consult on, prepare and publish a code of practice on standards to be followed in relation to the collection, processing, publication and other dissemination of personal data concerning children and pupils in connection with the provision of education services, which relates to the rights of data subjects, appropriate to their capacity and stage of education.

(2) Before preparing a code or amendments under this section the Commissioner must consult the Secretary of State and such other persons as the Commissioner considers appropriate as set out in Clause 124 (3).

(3) In preparing a code or amendments under this section, the Commissioner must have regard —
   (a) that children have different capacity independent of age, including pupils who may be in provision up to the age of 25, and
   (b) to the United Kingdom's obligations under the United Nations Convention on the Rights of the Child, and United Nations Convention on the Rights of Persons with Disabilities.

(4) For the purposes of subsection (1), "the rights of data subjects" must include—

   (a) measures related to Articles 24(3) (responsibility of the controller), 25 (data protection by design and by default) and 32(3) (security of processing) of the GDPR;
   (b) safeguards and suitable measures with regard to Articles 22(2)(b) (automated individual decision-making, including profiling), Recital 71 (data subject rights on profiling as regard a child) and 23 (restrictions) of the GDPR;
   (c) the rights of data subjects to object to or restrict the processing of their personal data collected during their education, under Articles 8 (child's consent to Information Society Services), 21 (right to object to automated individual decision making, including profiling) and 18(2) (right to restriction of processing) of the GDPR;
   (d) where personal data are biometric or special categories of personal data as described in Article 9(1) of the GDPR, the code should set out obligations on the controller and processor to register processing of this category of data with the Commissioner where it concerns a child, or pupil in education; and
   (e) matters related to the understanding and exercising of rights relating to personal data and the provision of education services.

7. Detailed aims of each part of the Code in Practice

The interpretative value of Recitals 38 and 71 among others, specific to children under GDPR, must be understandable for everyone in a data ecosystem. If not, uncertainty and unwillingness to cooperate in a responsible and interoperable manner, will make the whole process of children's data flows unworkable; and as today, makes it impossible for a school or child to manage their digital footprint.

7.1 Adherence to a code creates a mechanism for

a. controllers and processors to "*demonstrate compliance with the legislation or approved certification mechanisms."* [GDPR Articles 24(3)]
b. providers' confidence in consistent and clear standards, for the edTech sector
c. children, parents, school staff and systems administrators to build trust in safe, fair and transparent practice, so their rights are freely met through design and by default.

7.2 Schools give children's personal data to many commercial companies during a child's education, often for administration (such as absence tracking) and are not accessed by the child. It is rarely based on consent, Article 6(1)(a) or 8(1), but assumed, "*for the performance of a task carried out in the public interest*." A code should clarify any boundaries of this legal basis where it is an obligation on parents to provide the data, and what this means for the child on reaching maturity and later life, after education.

7.3 This should help companies understand "*data protection by design and default"* in practice, and [child] appropriate 'significant legal effect' (**Baroness Ludford, Second Reading** Col 144-5). The edges of 'public interest' in Clauses 17(1)(1) (transfers to a third country) and 9(2)(g) (special categories of data), will affect children in schools.

7.4 The draft amendment (2)(b) and (c) should both help children and those with parental responsibility, understand the effect of the responsibilities of controllers and processors, for the execution / limitation of their own rights.

7.5 GDPR states that child appropriate safeguards are necessary under GDPR Articles 13(2)(f), and 21-23 for exemptions. The Bill Schedule 1, Part 2 (5)(2) fails to set out those required safeguards designed for children.

7.6 Definitions of *"appropriate technical and organisational measures"* and what is expected to be *"appropriate to the risk"* for children under Recital 38 (children merit special protection) and UNCRC principles are needed. Small businesses and schools need information on acceptable and necessary levels of *"pseudonymisation, encryption, and on transmission"*.

7.7 Joint-controllers treat the same data differently. Schools need guidance on compliance where i) processing data under instructions from the controller(s) may differ from their own need and ii) there is a potential conflict in the best interests and restriction of the fundamental freedoms of the child, with regard to mass exports of school information management systems' and school census data, for re-use.

7.8 There is currently no obligation to register explicitly as a processor of biometric or special categories of personal data as described in Article 9(1) of the GDPR with the Information Commissioner or to publish policy regards notification of the data subject of the collection and processing of this category of data, its retention or destruction.

7.9 Further important rights that need addressed how to enact them across the sector, include those of GDPR Article 40:

(h) the measures and procedures referred to in Articles 24(3) (responsibility of the controller) and Article 25 (especially *"by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons")* as per Clause 55 (5) of the Bill, and retention periods, and measures to ensure security of processing (Article 32);

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations;

Subject Access rights are denied by the Department for Education today to children and parents wanting to understand their own national pupil data held by the Department today (ref. PQ108573). GDPR Recital 63 clearly states that a data subject should have the right of access to personal data, collected concerning him or her, at regular intervals, in order to be aware of and *verify the lawfulness of processing. (Case C-141/12)*. Every child and parent should understand who it has been given to. This improves digital understanding, data accuracy and data quality.

Note: 79% of parents if offered the opportunity to view their child's named record in the National Pupil Database would choose to see it. 9% would not and 12% not sure, according to a survey carried out of 1,004 parents in February 2018 by Survation[19]. The public do care about their personal data, and have a right to know.

[19] The independent survey results are yet to be published, carried out by Survation on behalf of defenddigitalme Highlights online http://defenddigitalme.com/wp-content/uploads/2018/03/StateOfData2018_infographicv10.pdf

8. Evidence from parents, children, and school staff in England, for the need for clarity, confidence and consistency in the schools sector

Parents have lost control of their digital footprint by the child's fifth birthday thanks to poor policy and practice at national and local level in education. Even though legislation in 2012 The Protection of Freedoms Act requires parental consent for use of biometrics and an alternative to be on offer, 38% of families were not offered a choice before use in practice according to a recent survey. There is an urgent need for parents and children to know which third-party systems use their personal data, to better understand their rights; and for schools and providers, to know and to meet their responsibilities.

8.1 Sample survey questions of 1,004 parents and their responses online between February 17-20, 2018[20]

The Department for Education has a database of over 20 million children's named personal records called the National Pupil Database. From there the Department can give children's data to third-parties. Have you been informed that the Department may give your child's data to third parties.	
My child's school has informed me of this	**31%**
My child's school has not informed me of this	**69%**

Regarding the use of the following, has the school offered you a choice whether to use this system or not *Base: respondents whose child's school uses any biometric technology **Base respondents whose child's school uses Internet Monitoring and keylogging software		
	Offered choice	**No choice**
*Fingerprints, retinal scans, palm scans or facial recognition (any biometric technology)	**62%**	**38%**
**Internet monitoring and keylogging software (software that records a child's Internet use)	**54%**	**46%**

Only 50% agree they have sufficient control over their child's digital footprint in school. A further 22% Don't know.

53% replied yes, their child has been signed up by their school to an app, technology, or online system that uses personal data. 24% Don't know. Of that 53% under a third were told if their child's personal data will be stored or transferred to third party organisations by the software.

81% of parents agreed or strongly agreed that parental consent should be required before a child's special educational needs data is shared for secondary re-use purposes with third parties.

8.2. Sample survey of 35 schools in England completed by IT staff with data protection responsibility [Link to the IT staff survey responses]

8.3. Further similar evidence is available on request, from research with every Local Authority across England and Wales, with responsibility for education (formerly known as Local Education Authorities) -- as well as various organisations across Scotland and NI.

[20] Ibid see ref 19