defend|digital|me

The STATE of DATA 2018

Lessons for Policy Makers

A review of children's privacy and data protection in state education in England with a view to the UK Data Protection Bill and General Data Protection Regulation

This interim report is a summary of highlights with recommendations for policy makers, selected from work-in-progress *The State of Data 2018: Right and Responsibilities. A review of children's privacy and data protection in state education in England with easy steps for GDPR*.

While the bulk of our work is related to England, data protection is for the most part, not devolved, unlike education. There are differences in law as regards children's age and capacity, which are reflected in GDPR and the UK Data Protection Bill (as of May 2018). However this makes no material difference in our comments. Our general recommendations and technology apply across the UK unless otherwise stated.
The National Pupil Database is that containing children's personal data from England.

Wherever we refer to *the Survation poll, our poll* or *our survey*, we mean the State Of Data 2018 survey: A poll of 1,004 parents of children age 5-18 in state education in England, carried out between 17-20 February 2018 by Survation, commissioned by defenddigitalme.

As there has been no more authoritative data collected on the demographic make up of parents in England with children age 5-18 in state funded education, data were not weighted.

Full tables and its methodology can be found online at: http://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables.pdf

May 2018 v2.1

About defenddigitalme and what we do

We are a non partisan civil society organisation. We campaign for safe, transparent and fair use of data across the education sector in England. This report work was funded as part of an annual grant 2017-18 from the Joseph Rowntree Reform Trust Ltd. for whose continued support we are very grateful.
defenddigitalme | Registered company number 10768509 | ICO registration ZA267313

defenddigitalme.com

Contents

Is 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) sufficient?

YES 50%

Don't Know 22%

NO 28%

If you had the opportunity to see your child's named record from the National Pupil Database, would you choose to see it?

YES 79%

Today the Department for Education refuses children and parents the right to see their own record, check it is accurate or have data corrected. defenddigitalme is campaigning to have that changed, and wants the government to respect children's Subject Access Rights and Recital 63 in the General Data Protection Regulation

Executive summary

The government sets out its aim in the Digital Charter[1] to give people more control over their personal data through the Data Protection Bill and protect children and vulnerable adults online. We suggest that this must start in education by ending bad practice, and building better data practices founded on rights.

This research from defenddigitalme explores how parents in England think their children's data are used in education and their attitudes and trust in some of the uses children's data are put to at national level. We asked whether or not their child had been signed up to or involved with a range of everyday technologies in use in the UK education sector.

We also highlight some of the key issues in some of the most common technologies used in schools and in collections of national pupil data.

This is an interim summary report for policy makers based on our research. It highlights:

- Parents have lost track of their child's digital footprint in school by a child's 5th birthday.

- A quarter of parents in our survey[2] say they don't know if their child has been signed up to use any technology by their school at all.

- Before a child has left primary school aged 10, their personal data are commonly sent to
    - over ten commercial companies without a parent's knowledge — often shared onwardly as is, or after processing, with many app and platform partner affiliates who go on to use data for profiling behaviour, or for product marketing purposes;
    - sent over 25 times in national school censuses and attainment tests in England, to an ever growing National Pupil Database of 23 million named records for re-use for life,
    - and are given away to thousands[3] of data analytics researchers by the DfE.

- While parents give the Department for Education (DfE) a high level of trust to use data well (68%), almost the same number of parents (69%) said they had not been informed the DfE may give out children's data from the National Pupil Database to third parties.

- In Scotland and Northern Ireland children's sensitive biometric data need improved protection in law, since the Protection of Freedoms Act 2012 (E&W) does not apply.

- Web monitoring software, common in England's schools since 2016, scans and profiles children's every Internet search, surveils their screen content and if a child types a keyword that matches a watchword in libraries of up to 20,000 words. automated flags are created on permanent records. One latest version enables IT admin operators to see a child through the webcam. Schools also impose the software on personal devices in school, so operate at home, in personal space and time. Child safety and rights demand review and regulation of these policies and software, and safeguards are necessary on profiling and automated decision-making, to create protections against harm, and ensure children's flourishing.

[1] https://www.gov.uk/government/publications/digital-charter/digital-charter#approach

[2] StateOfData2018 survey: 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

[3] PQ 120141 Answered by the Rt Hon Nick Gibb on 18 January 2018 asked by Layla Moran MP www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-12-18/120141/

Recommendations for Policy Makers

While DfE's advice for schools in England and Wales how to start to prepare for GDPR[4], published on April 23, 2018, is welcome, it is only that — advice, restricted in its geographical scope, and only for schools' own readiness. 28,000 schools across the UK do not have the capacity or clout to do what is needed to bring about necessary changes in supplier practices. Every child's data rights in the UK should be treated with consistency and fairness. This is why we believe a UK wide Statutory Code of Practice is necessary, and would give controllers and processors, schools and suppliers, a concrete way to "demonstrate compliance with the legislation or approved certification mechanisms," as set out in GDPR Article 24(3).

There is no time to waste for improvement in children's knowledge about data and digital rights. It is already 5 years since the 35th conference of European Data Protection and Privacy Commissioners urged member authorities in 2013 to adopt a common programme on digital education, with the aim of the promotion of digital literacy.[5] Where better would this fit than Personal, Social, Health and Economic education?

Children can't put growing up on pause, while policy makers get their act together. To better protect children and uphold their data rights and human rights, defenddigitalme recommends:

- National pupil databases must be safe, and children's subject access rights assured
- Safeguards on profiling and automated decision-making with significant effects
- Obligations on controllers and processors of biometric data to explicitly register processing of this category of data with the Commissioner where it concerns a child
- A Statutory Code of Practice in Education to underpin and enforce good practice, bringing clarity, consistency and confidence to data handling across the sector, and promoting children's rights under the UN Convention on the Rights of the Child.
- Education in schools and teacher training on data and digital rights and responsibilities

A child's freedom to develop and the ability to flourish depend on how we respect and enact their rights. Article 16 of the UNCRC6, specifically enshrines that, 'No child shall be subjected to arbitrary or unlawful interference with his or her privacy'. Children need a rights-based approach in applying law, since schools can almost never process children's personal data based on consent Article 6(1)(a) or 8(1), but "*for the performance of a task carried out in the public interest.*"

Today, digital policy for children at government level is presented almost exclusively in terms of child protection, underpinned by a simplified view of complex and conflated risks as online stranger-danger, screen-time and access to harmful or offensive content. But the scale of children's, staff and parents' data harvesting in education is monumental. The datification of children and their commodification by commercial companies is shocking, during *loco parentis* of state education, outwith parental oversight and consent. This lack of care is negligent.

National, regional and local data policy and practices can no longer ignore children's rights to privacy, participation, and the protection of their digital footprint.

---

[4] Guidance to support schools with data protection activity, including compliance with the General Data Protection Regulation (GDPR). https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

[5] DPAs recommend digital education http://www.privacyconference2013.org/Declaration_and_Resolutions_adopted_at_35th_International_Conference

[6]UNCRC https://downloads.unicef.org.uk/wp-content/uploads/2010/05/UNCRC_united_nations_convention_on_the_rights_of_the_child.pdf

Digital understanding and education

The Children's Commissioner believes, "We are failing in our fundamental responsibility as adults to give children the tools to be agents of their own lives."[7] (Growing Up Digital, 2017) Companies often push back the responsibility for safe data use to children under flawed notions of 'informed consent'. Education on rights goes hand in hand with enforcement of supplier responsibilities. Policy Makers should enable this digital understanding in education.

Children and young people need agency in everyday digital interactions according to their capacity as they mature. Understanding how our personal data are used by others makes a difference to the balance of power in common interactions with companies and the state. That balance is vital to maintain if we are to be able to remain in control of our own lives, with self determination, to make informed choices, see or object to discrimination, and understand interferences with our democratic rights. Human rights must stay central in a world in which decision-making about us, is becoming ever more machine-led without us.

Our children's full development and flourishing may be supported by, but may also be limited by, data about them; through labels given to them for life or compromise of their digital footprint in school. If children and parents are not told how their data are used, we cannot identify risks or protect against them. National school data are used for targeted interventions by the Home Office. Young Offender labels have just been added to the Alternative Provision 2018 census, and in parallel research is going on using national pupil data in predictive modelling at a criminology institute,[8] and research linked to Police National Computer Data.[9]

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

Statutory code of practice in Education

Lord Knight at the Second Reading of the 2017-19 Data Protection Bill in the House of Lords, spoke out for schools, saying[11]: *"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."*

While existing Data Protection law should have served as a deterrent to bad practice, it has not been enough without statutory safeguards of rights, a clear Code of Conduct for practice, or enforcement.

More clarity, consistency and confidence handling data are needed in the education sector. Article 25(2) of the GDPR is perhaps one of the most significant for schools and their suppliers — data

---

[7] Growing up Digital (2017) p3 [archived copy stored on defenddigitalme website accessed March 1, 2018] http://defenddigitalme.com/wp-content/uploads/2018/03/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf

[8] Predictive modelling using national pupil data from the Cambridge Institute of Criminology http://defenddigitalme.com/wp-content/uploads/2018/04/Cambs_Crimi_NPD.pdf

[9] Police National Computer Data case study http://defenddigitalme.com/wp-content/uploads/2018/04/PNC_NPD.pdf

[10] Council of Europe Strategy for the Rights of the Child 2016-21 Para 37, p15/36 https://rm.coe.int/168066cff8

[11] Data Protection Bill Second Reading, 10 October 2017 Hansard, Lord Knight of Weymouth https://goo.gl/cxSZXM

protection by design and default. But what that means in practice for the rights and responsibilities of schools, staff, parents and children, will not be realised through only guidance to schools.

Without enforcement it is unlikely that we will see improvement on current practice. How will schools know what appropriate technical and organisational measures are? Without knowing the expected standards for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed, data collection will continue to be excessive. Obligations apply to the amount of personal data collected, the extent of the processing, the period of storage and accessibility. 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 (25)(2).

Schools and industry partners need clarity to have confidence that they can buy, sell and use tools safely with consistent standards, and with children's rights at the heart of their design. Children need Statutory support of their rights written out tailored to their needs and capacity, for the complexities in education.

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

- Clarity in expectations from suppliers what can and cannot be done using pupil data in schools, especially on the boundaries of public and legitimate interests, profiling, data analytics, product development, 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.

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) on the preparation of codes of conduct incorporating safeguards for children." How this should be respected would be set out and enforceable.

The International Working Group on Data Protection in Telecommunications summed up in their Working Paper on e-learning platforms in April 2017:[12] "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."*

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."* [13]

[12]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

[13] https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/130.pdf Paragraph 353, Growing up with The Internet, March 2017

What a Statutory Code of Practice in Education could include

“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 123 (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.

Profiling and automated decision-making and the public interest

Given that "such a measure should not concern a child" is only in a recital, there is a need for data controllers and processors to understand GDPR recitals 71 and 38 with a degree of interpretation. However, little attention is paid to the rights or specific profiling experiences of the child. We believe clearer and enforceable guidance and standards on children and profiling and automated decision-making are needed in practice. The Working Party 29 also recommended such a code.[14]

There are hard questions to answer in schools of the edges of *the public task* and what are *automated processes with significant effect*. Cashless payment systems that interact with or without biometric readers may be core to a school's administration convenience, but are they part of a public interest statutory requirement? And if so, what happens if a parent or child objects to the app? A ten year old can be signed up by a school to over ten apps that use their personal data, transfer it abroad, process for marketing and pass onwards to other third-parties without the child's or parental consent or knowledge, by the end of primary school. All without any oversight or minimum standard safeguards.

Under the GDPR, individuals have a right not to be subject to decisions based solely on automated processing of their personal data, including profiling which produces (i) legal effects concerning them; or (ii) a similarly significant effect. It does not define either 'legal effects' or 'similarly significant effects.' Where in practice does predictive scoring of attainment by third party companies fit and on what basis? Sold to schools, some Heads post scores on staff room walls and target interventions with a handful children who will raise or lower the school's overall performance outcome.

Leckie, G., & Goldstein, H. (2017) concluded in their work on the evolution of school league tables in England 1992-2016: 'Contextual value-added', 'expected progress' and 'progress 8' that, "*all these progress measures and school league tables more generally should be viewed with far more scepticism and interpreted far more cautiously than they have often been to date*.[15]

Baroness Ludford was one of many peers to point out difficulties in the House of Lords during the Second Reading of the UK Data Protection Bill, on October 10 2017[16]: *"We may need seriously to look at the lack of definition of "substantial public interest" as a basis for processing sensitive data, or even of public interest….There is also concern that the safeguards for profiling and other forms of automated decision-making in the Bill are not strong enough to reflect the provisions of Article 22 of the GDPR. There is no mention of "similar effects" to a legal decision, which is the wording in the regulation, or of remedies such as the right of complaint or judicial redress."*

Claims of 'public interest' from the State can be far reaching, and well beyond reasonable expectations and the original purpose of data collection at local and national level. Our research into school census expansion plans[17] to start to collect nationality data in 2016, revealed an agreement for monthly handovers of children's national pupil data for immigration enforcement. This impinges on fundamental rights to privacy and the data protection principles of purposes limitation, and fairness.

In July 2015, the Department for Education and Home Office Border Force Removals Team agreed a Memorandum of Understanding[18] to share pupil data including names, date of birth, gender, home

---

[14] Working Party 29 profiling and Automated decision making http://defenddigitalme.com/wp-content/uploads/2018/05/wp251rev01_enpdf-1.pdf

[15] Leckie, G., & Goldstein, H. (2017). The evolution of school league tables in England 1992-2016: 'Contextual value-added', 'expected progress' and 'progress 8'. British Educational Research Journal, 43(2), 193–212.

[16] http://hansard.parliament.uk/Lords/2017-10-10/debates/22188EC1-6BAB-4F06-BE64-5831ABAF78E2/DataProtectionBill(HL)

[17] 2016 school census in England http://defenddigitalme.com/wp-content/uploads/2017/08/Briefing_pupildata_BorderForce_Nationality.pdf

[18] Memorandum of Understanding between the Home Office and Department for Education obtained via Freedom of Information request https://www.whatdotheyknow.com/request/377285/response/941438/attach/4/20151218%20DfE%20HO%20Final%20V0%201%20REDACTED.PDF.pdf

address and school address for up to 1,500 children a month, from the last 5 years of their records, for various purposes of direct interventions. There was no public consultation or announcement of this. Version 1.0 was valid from July 2015 until October 7, 2016 a day after the start of a new collection of nationality data in the 2016 expanded school census. In October 2017, the Department for Education confirmed in an interview with Sky News that, information obtained from the National Pupil Database was used to contact families to "regularise their stay or remove them."

At the time of writing, in May 2018, the DfE has still never told schools at all, that it is using any national pupil data for Home Office purposes of immigration enforcement. There are unconfirmed reports that after a successful #BoycottSchoolCensus campaign, and over 25% non-return rate, the collection of nationality and country of birth data will end. The monthly data handovers continue.

In general, if such processing should not routinely concern a child (GDPR Recital 71) and children should be recognised as vulnerable and require special protections (Recital 38), there will need to be change and very strong codes of practice and enforcement in England, to respect the intent of the GDPR, this WP29 guidance, and CoE Principle 3.5,[19] "*profiling of persons who cannot freely express their consent be forbidden, especially, for example, adults with incapacity and children, within the meaning of the UNCRC.*"

Recommendations on profiling and accountability under the GDPR

- Data protection and privacy safeguards by design are required to prevent harm from profiling, with appropriate technological and organisational measures. (Article 25)
- Accountability measures that routinely profile a child require human safeguards to be built into the process so that any errors are easy to identify, the outcomes easily understood by the staff and parents, and any effects as a result explained to both. Right to explanation must be offered by schools to every pupil and parent. (Article 12-15) (Article 22(2)(b))
- Children and parents have at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. Test results must be made available to pupils and families and cannot be carried out and results black-boxed. (Article 22(3)
- Where profiling includes ethnicity and disability or other SEN health related categories of data, it must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. (Article 9(2)(g) Article 22(4)).
- Privacy and Data Protection Impact Assessments should be carried out and published before any national test, new data collection or new processing is approved, especially where it concerns profiling. The assessment should be independent from the data user groups and be published in public consultation. (Article 22(2)(b)) There was no privacy or human rights assessment of national pupil data collections since they began in 1996 [See pp29-30].
- Indefinite retention of pupil level data and profiling children at pupil level with a view to interventions, merits special attention of regulators, particularly in predictive modelling use and research exemptions.

[19] CM/Rec (2010)13 adopted by the Committee of Ministers on 23 November 2010

Risk and harms from profiling and automated decision-making

When contextualising children's right to privacy among their other rights, best interests and evolving capacities however, "i*t becomes evident that children's privacy differs both in scope and application from adults' privacy.*"[20] This must mean extra consideration should be given before profiling decisions are recorded, kept and used to make decisions because profiling as a child can have lifelong implications if used for interventions at school [21], in insurance discounts[22], potentially in screening for university[23], for recruitment marketing[24], or future employment.

Strong data protections can also minimise exposure of knowledge about children to third-parties, that can be used for bullying, grooming, blackmail, or put vulnerable children-in-protection at risk of being found.

Schools and learning-tool providers are not required to demonstrate the pedagogical quality or evidence of learning benefits of apps, above and beyond other tools. There is no accountability for any unexpected side effects, or trade off between the cost-to-a-child of their right to data privacy and freeware that may be appealing to schools with tight budgets.

Commercial products are widespread in schools, sold as ways of reducing workload and increasing efficiency through reduced administrative time. Many are free to schools, but offer premium in-app paid content to parents and pupils over time, or other secondary services such as private tutoring. There is no oversight or accountability for the ethical or privacy effects of education technology.

Ease of access to freeware technology has far outstripped staff and parental knowledge of their data rights and responsibilities, and how easy it is to understand how data are used. Profiling is routine. But there can be no meaningful interventions by a teacher to know if the attainment profile is accurate upon which they decide to intervene, or not. Whether the wellness app that suggests a mental heath concern on a teacher's dashboard is accurate or quackery; or how an AI designed seating plan [25] decides which behaviour does or does not merit separating friends, or arranges a room, and has it right.

There is also a risk that increased reliance on machine-made decisions, may mean teachers trust their human opinion less and miss out the children, with whom they might otherwise have decided to act.

DfE registered self certified third-party app or providers, are not barred from enabling targeted marketing to children, despite recognising in its current DfE cloud guidance (2014), that, "*there are obvious difficulties with schools deciding if children are competent enough to understand any explanation of their data being used for advertising."* [26]

Children are exposed to increased risk of price discrimination or ad targeting on their own personal devices or personal time and home computers, through school imposed platforms and apps. Interactions with children's mobile phone and accounts for websites created in school, leave behind a data trail for companies to follow children home through permanent cookies and their online activity.

Companies then track children and profile them to learn about their behaviours, locations and likes, to target advertising or tailor content to grab and keep their attention, which is valuable in advertising and how many websites make money.

---

[20] Privacy, Protection of Personal Information and Reputation - United Nations Children's Fund (UNICEF) (2017) https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf

[21] Research by the Cambridge Institute of Criminology using pupil data for interventions with 40 schools in London http://defenddigitalme.com/wp-content/uploads/2018/04/Cambs_Crimi_NPD.pdf

[22] US State Farm Insurance Good Student 25% discount for 'good grades' https://www.statefarm.com/insurance/auto/car-insurance-for-teens (April 2018)

[23] I was rejected from University because of my record, Inside Time, April 3 2018 https://insidetime.org/i-was-rejected-from-university-because-of-my-record-now-im-campaigning-for-fair-treatment/

[24] Schools Week MoD requests sensitive pupil data by mistake https://schoolsweek.co.uk/mod-makes-inappropriate-request-by-mistake/

[25] Class Charts https://www.classcharts.com/

[26] DfE Self certification scheme for school cloud providers https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644845/Cloud-services-software-31.pdf


School

At local level schools expose children's data throughout their school life to:

- Platforms, like Google's G-Suite in education, that give children personal email accounts, often with external access, and enabling social log-in to apps, that track every Internet use and target ads on YouTube. Core services and Additional services operate different terms and conditions, but there is no meaningful consent process because schools do not offer a real alternative to using the platform, and parents feel compelled to say yes even if asked, which most schools do not do, or bundle into a multiple page school-home ICT agreement.

- Loss of autonomy and rights: Schools export class or school-wide populations of children for named accounts for administrative purposes in a few clicks in bulk transfers at speed out of the school information management system without processes to adequately assess risk, minimise data transfer, or inform parents or children.

- Hidden tracking systems: in May 2017 an education technology blogger revealed Edmodo, a US based education platform, exposed students and teachers to targeted ad tracking. Once he made it public, the company removed the tracking that he observed and discussed in his post, and he wrote, "Their response was fast, and they deserve a lot of credit for making this decision, and implementing it quickly."
  [Bill Fitzgerald, https://funnymonkey.com/]

- Loss of data through leak, misuse or theft: Edmodo was later hacked and lost 77 million staff and student records from 550,000 schools worldwide, 2 million of the records were UK accounts. Third party school information management systems commonly appear weak in supporting data rights, by design. When we asked IT professionals asked if schools perform any regular data audit from the pupil information management system, few said yes. 40% said they did not because the pupil information management system does not offer this functionality, in addition to the other 40% that simply replied no. This means there is no oversight of access to, or traceability of pupil data, and on reaching adulthood, children have no way to regain their own digital agency.

Apps can access children's personal data at rapid speed and scale

Apps[27] for administration are everyday for homework tracking[28], school-home communications or sickness and absence reporting. Cashless payment systems store parents' financial details and are sent children's personal profiles from school information management systems in bulk, school-wide.

Apps can be sent special educational needs data, and then used to record classroom behaviour points, creating permanent behavioural profiles. The Times,[29] Guardian, and Daily Mail reported in the last week of April, that US based Class Dojo harvests data on how British schoolchildren behave. Where are the tests for pedagogic value, health and safety, privacy and ethical regulation and oversight?

The Department for Education should ensure each school information management system provider can demonstrate it offers data audits and adequate ability to audit, correct and remove data in schools and enable adequate controls on the release of data in bulk or at individual level— that MIS providers cannot today demonstrates their failings in current data protection law and should not be fixed by charging schools — processors must also be compliant.

In February 2018, a researcher in Australia found that children's identifiable data were publicly available to download from the app Mathletics. Not only did the app harvest personal data, but exposed it worldwide. It is widely used in UK schools and exposed over 170,000 children's details.

The app privacy policy states that the company retains the personal information that they collect from and about our registrants for as long as it is needed to provide access to the site or to manage that Registrant's account. It also states that teachers can opt out of this retention.

"*The opt-out option for 2017 has now closed"*. This means children's personal data with the company according to its internal plans may no longer be withdrawn. It is therefore unlikely this app can be used lawfully since schools will find a consent basis hard to apply in school and parents and pupils are unable to object to the app continuing to process their data. In our opinion, this app is processing in

[27] Hackers steal Edmodo users' details https://schoolsweek.co.uk/hackers-steal-edmodo-users-details/

[28] Show My Homework / Team Satchel https://www.teamsatchel.com/product/smhw.html

[29] The Times, ClassDojo is harvesting data on how British schoolchildren behave https://bit.ly/2jpMl5G The Guardian ClassDojo: do we really need an app that could make classrooms overly competitive? https://bit.ly/2I9vy4E Daily Mail Parents fear app is storing private data in the US on how their children behave https://dailym.ai/2HFX4mP

ways incompatible with data protection law under the GDPR, and how it can be applied in education.

Under GDPR, accountability for data management, knowing where children's data have gone, may seem arduous if schools have not done so before now, but simply means processes to date have not been compliant with existing Data Protection law in place since 1988. Data controllers and processors will need to have registers in place to be able to identify and audit which data leave the school information management system and know whose data goes to which third party.

There are also questions over data minimisation and excessive data transfers to consider. Most APIs do not appear to be able to restrict distribution of bulk data extractions at a pupil level, and can only enable data limitation at a data group level, for example 'names', but not limit to first and exclude only *las*t name. All data do not have the same levels of sensitivity, and while special categories of data exist under GDPR to assign special recognition and rights to, these are largely ignored in edTech systems.

In other contexts for example, labels under special educational needs (autism, mental health) and reasons for exclusion (theft, violence, sexual misconduct) would be inferred to be revealing especially sensitive data, health and criminal convictions. The contexts are different, but are the implications?

Department for Education guidance to schools suggest that the child's unique pupil number or UPN is a 'blind number', and not an automatic adjunct to a pupil's name and only transferred to those with a genuine right and requirement for its receipt. But apps tend to ask for this number, and they are exported at scale and speed. 2013 issued guidance on UPN distribution stated, "The data protection restrictions associated with UPNs mean that it is only possible for UPN data to be shared by CTF between schools/ academies, Local Authorities, DfE and other prescribed government departments. Under the Data Protection Act 1998, the UPN is designated as a 'general identifier' making its use for any purpose unrelated to education illegal. A pupil's admission number, rather than the UPN, should be used as the general pupil reference number on the admission register or paper files." A December 2017 update, waters this down.

A transparent organisational framework in which to research where a child begins their digital journey within the education system is missing. There is no easy way for a child or parent to understand the structure of the state education system, and therefore what flows of data exist between those organisational units. It is impossible for an individual to understand on their own where their personal data flow, who controls and processes it, or to keep up with any loss and leaks. Using apps introduces hundreds of more points of distribution, and puts the onus on schools to ensure documentation.

When talking about children's data protection and data privacy rights, with children or their parents, we cannot do so without informed understanding how much data and what types of data are collected on children in schools, or how data are used, for what purposes, and by whom.

Yet a quarter of parents in our survey of 1,004 parents[30] say they don't know if their child has been signed up to any technology by their school, and only 50% say they have sufficient control of a child's digital footprint in school. Most schools do not share app or platform policies with children or parents. Privacy notices fail to communicate any meaningful understanding of local or national level data uses. 47% parents in our survey say their schools use an app for behavioural monitoring and profiling.

As the volume of data collected about children has grown, educational settings have not maintained their own knowledge how data are used or kept up with informing parents and children where their data go, or in decision-making over its collection or use. Often staff themselves simply follow instructions and trust the purposes of any new statutory collection, without question. Little information trickles down to the administrators who submit national data and even less to families.

The legal basis for data collection is rarely asked before it begins. Do these data form part of the child's core educational record or not? Are they necessary and proportionate and use only the minimum amount of data? Is there a balance between the necessity of use and an individual's fundamental right to privacy? Parents and children must be informed at minimum pre-data transfer.

Data protection best practice is not always aligned with the data controller's notion of reasonable or ethical expectations of privacy especially where their business model depends on data exploitation.

Data Protection laws intended to protect pupil data held by or for schools are simply inadequate without enforcement, to address the challenges of today's digital age and the rate of growth of commercial third-party technology adopted in schools without oversight or transparency. A Code of Practice is required.

[30] StateOfData2018 survey: 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

Biometrics in schools

The use of biometrics in UK schools began in 2001 with fingerprint technology as a means to identify children borrowing books from a school library. Biometric processors now profile everything a child buys in the canteen, books read in the library are rated with points assigned for high read-word counts over time. Behaviours are recorded, monitored and dashboards drawn.

It is possible to transfer biometric (numeric) data from one database to another. There are interoperable programmes that can do this established by National Institute of Standards and Technology (NIST) according to Pippa King of Biometrics-in-Schools.

In May 2013 she sent every police force in the UK a Freedom of Information request asking if that force had ever accessed a school biometric database:

- 4 forces failed to answer the request (8%)
- 2 forces answered stating they had no information (5%)
- 4 forces stated no they had not accessed a school biometric database (8%)
- 38 forces refused to answer citing cost (79%).

It is left unknown if school biometric database data has been transferred from a school database to another biometric database or whether data has been scanned from a school biometric database.

Uniquely Britain was the first country worldwide to introduce biometric technology into schools in 2001 and its uses are expanding, also now in Scotland[31].

UK schools use biometric data in various technologies —

- fingerprint
- iris scanning
- facial recognition
- infrared palm and infrared fingertip scanning

— all of which were introduced in schools quite often without the consent or even knowledge of the pupils' parents/guardians. The Protection of Freedoms Act 2012 required schools to obtain the consent of parents and children (under 18) to process and store students biometric data. But our poll still found 38% where the school was already using biometric technology, had not been offered any choice.

The same rights that are afforded to children in England and Wales with regard to consent to educational establishments taking and processing their biometrics do not apply to children in Scotland and Northern Ireland. The Protection of Freedoms Act applies only to England and Wales.

[31] Edinburgh high schools roll out fingerprint scanning to pay for lunches, May 3, 2018 http://www.heraldscotland.com/news/homenews/16201636.High_schools_roll_out_fingerprint_scanning_to_pay_for_lunches/

In December 2016, Biometrics-in-Schools sent Freedom of Information Requests to 216 secondary schools in Northern Ireland, Wales and England. Only 103 (47%) schools provided answers, including copies of privacy notices about pupil data usage. Based on those FOI responses examined for this report, 57% of secondary schools that replied, used a biometric system, and 37% used biometrics for more than one application. Our commissioned poll of parents[32] in February 2018, suggested at secondary school that is closer to 70%. We found that 50% of parents where biometrics systems were in use, had not been informed for how long a child's biometric data would be retained.

Informed parental consent is absolutely necessary and required under the Protection of Freedoms Act 2012. Parents and children need to be well informed how biometric data processing of all kinds work, and potential consequences of a breach. Biometric system introductions must be with an active process to opt-in, not make parents have to go to extraordinary efforts to opt-out.

Leaton Gray and Phippen (2017) found that, "*pupils were not inducted into biometric systems in the same way that they had been in 2006 when such systems were relatively novel.There were no talks on the purpose of the system and related data privacy issues (indeed we found that data privacy was not mentioned at all other than in the context of e-Safety.)"*

Frustration of use in the systems was summarised by the researchers, in four areas: Pupil resistance, Pupil mistrust, Hygiene and Parental surveillance. And while we agree with their assumption that school staff intentions where these technology are employed are benign, we also support their finding that there was no reflection on the potential future impacts, "*staff and pupils are persuaded by the convenience of such systems to a point that they do not reflect on the potential social harms, or related legal issues. Schools did not have effective data protection policy or practice in place to be able to manage data such as biometrics effectively and in a legally compliant manner."*

Biometric data in library, print, locker and canteen service use based on fingerprints, profile children's biometric data and children's activity down to the nth degree, even to what they buy and its nutritional content. Records of 'consumption' which are actually records of spend, are sent to parents. At what point of maturity should a child have the right not to be profiled for parental oversight, and where does well-being stretch beyond necessity, into curiosity? Where these systems are in use, 38% of parents replied in our poll that they had not been asked for consent or offered an alternative system to use.

Processing of biometric data is a high risk for rights, yet its use is casual and everyday for identity systems and basic administrative tasks in the canteen, library, locker and building access. Safe use of biometric data and big data analytics by state and commercial sector in education needs stronger enforcement of responsibilities and rights on data processing, and in particular regards profiling.

Biometrics has grown exponentially without any according increase in the regulation or oversight who can collect such sensitive data and why. From discussion with parents, we believe discrimination against those who opt out of its use in canteen services is already common, in so far as many schools fail to offer any alternative to its use, and therefore deny access to hot meals, including FSM children who are therefore bound to use the system. But there is little national research, where these systems are in place, and no requirement for use to be registered explicitly with the Information Commissioner.

Ethical use of voice systems using AI in the classroom are also a new area of biometric data collection that needs consideration. These systems are not designed with children in mind, and their voice data, vocabulary and interactions may be unexpected. In February 2018 Alexa users reported their machines emitting unexpected laughter-like and whistling noises without being prompted to wake.[33]

"The basic knowledge and understanding necessary to navigate an AI-driven world will be essential," commented the House of Lords Select Committee on Artificial Intelligence report, *AI in the UK: ready, willing and able?* Published in April 2018[34] it recommended that the ethical design and use of technology becomes an integral part of the curriculum. We can only achieve that, with a foundation of knowledge of data about us and the world. The foundations of an AI-driven world are built on data. In a world of increasingly machine-made decisions, it is vital to restore and uphold human rights.

---

[32] #StateOfData2018 survey: Survation poll of 1,004 parents of children age 5-18 in state education in England, carried out between 17-20 http://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables.pdf

[33] The Verge, Amazon has a fix for Alexa's creepy laughs February 2018 Shannon Liao https://twitter.com/i/moments/971424274731950081

[34] *AI in the UK: ready, willing and able?* House of Lords Select Committee on Artificial Intelligence (April 2018) https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf

If every child is to flourish in society, they must be empowered to cope in a digital environment, and systems must be designed in such ways that risk and harm are minimised, and human intervention mitigates those the automated decision making miss.

New technologies are pushing the boundaries of what is possible, and are at the opposite end of the scale compared to levels of understanding of what happens to children's data in schools, and data security.

CCTV can now also be used for facial recognition and some commercial systems are starting to combine facial scanning, with identity systems, to sell as solutions for pupil registration. [35]

Yet only half of parents in our survey, said they have been told how long school CCTV images are kept today, and in February 2018, Infosecurity Magazine[36] reported that the ICO has launched an investigation after it emerged that CCTV footage from several Blackpool schools was live streaming on a US website.

Lord Lucas has asked practical questions in debates on the UK Data Protection Bill, that businesses need to know about technology implications in the GDPR, including, "*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?"*[37]

There will no doubt be confusion in providers that operate the same app or platform for both educational and home markets. In schools, if data are collected in the performance of a public task, data are not collected on a consent basis. Yet on home apps, parents will be asked to approve the collection of personal data from their child under 13, through age verification (Article 8(1), if the system is targeted *at* a child and accessed *by* the child. It will inevitably mean some apps used in school will start asking for parental age verification during the sign up process even though schools are not processing on a consent basis. At the time of writing, how this will work in practice is unclear.

Will Recital 57 and data minimisation be strong enough principles to protect from excessive data collection in the name of age verification, when in fact all AV demands, is a check of attributes?[38]

Many child rights advocates question "*the short-sightedness of policymakers in using data protection regulation to encroach into broader social and developmental issues*," and ask why young people themselves have not been given the opportunity for consultation and involvement in shaping the new data protection law and to understand how it will affect them.[39] While children should be involved in questions of how their data are used, there is no such thing as a general digital age of consent under GDPR, a common mythunderstanding. Children cannot generally meaningfully consent to their own data use in the public sector and parents should not only be included, but are required to give active consent for biometric data processing. We must also ensure that improving digital capability is not another area where those with special educational needs are disadvantaged.

In summary, everyone working in the education sector including policy makers, sets high store on child safety and the values encapsulated in Article 24 of the Charter of Fundamental Rights, *in all actions relating to children, the best interests of the child must be a primary consideration*. However, inadequate technical knowledge how data are used, coupled with opaque systems-by-design, means staff and parents alike don't see how much children and schools are revealing to third-parties about children's lives and can inadvertently put them at risk of harm, or restrict their development. Enforceable guidance and common expectations of ethical as well as lawful practice are needed. Without changes in suppliers' design and approaches to what is a permissible level of child exploitation in their business models— if any; change is unlikely, and children will continue to be exposed to risk.

[35] As seen at the Bett Show 2018 exhibitor https://www.bettshow.com/bett-products-list/edureg

[36] Infosecurity Magazine, Muncaster, P. (2018) https://www.infosecurity-magazine.com/news/school-cctv-streams-end-up-on-us/

[37] Second Reading, Data Protection Bill House of Lords, October 2016 Lord Lucas [Hansard] https://goo.gl/723xfc

[38] Age Verification as the new cookie law? Booth, P. (2017) http://www.infiniteideasmachine.com/2017/08/age-verification-as-the-new-cookie-law/

[39] EU General Data Protection Regulation Article 8: Has Anyone Consulted the Kids?, Savirimuthu, J., Senior Lecturer in Law at the University of Liverpool, http://blogs.lse.ac.uk/mediapolicyproject/2016/03/01/eu-general-data-protection-regulation-article-8-has-anyone-consulted-the-kids/

Web monitoring: profiling and automated decision making

Children and young people should not find that software in place for their safeguarding, causes them lifelong reputational risk and real harm. Yet this is the result for some children wrongly labelled as at risk of suicide or gang membership. In England web monitoring and filtering includes profiling through keyword logging and real-time screen recording of all Internet use, both in school and at home, 365 days a year on school provided laptops or software installed on personal items in bring-your-own-device policy. While systems providers have been around for several years, use is even more widespread after statutory guidance introduced in September 2016 on 'safeguarding in schools'.[40]

The opinion of the Working Party 29 2(2009) noted, *"It should never be the case that for reasons of security, children are confronted with over surveillance that would reduce their autonomy. In this context, a balance has to be found between the protection of the intimacy and privacy of children and their security. Legislators, political leaders and educational organisations should, in their respective areas of competence, take effective measures to address these issues."*[41]

Content monitoring and data harvesting are without children's or parental understanding and without oversight of error rates, independent assessment of cost and benefit, or clear standards or course of redress. Parents and children may sign 'school-home ICT agreements' but consent is manufactured and fail to set out how systems work, their consequences or meet fair processing of data protection law. In over 400 policies, we have seen none that explains to young people how these systems work.

This 'normalised' surveillance software on children's school and home computers, bring-your-own-devices and in personal spaces and private time is highly invasive into private and family life. Every keystroke is monitored and some check against libraries of over 20,000 watchwords. Many offer multilingual versions. Every screen is captured. Some providers even permit the IT admin to operate the child's web camera remotely. It is impossible in some schools for children to get errors removed. *"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.*" [42]

Notes can be held on record indefinitely, shared with Prevent and police, and show up in the statistics.

The undefined "authorities" are notified, if someone tries to browse to one of an unknown and changing set of websites, 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 of websites and keywords come from a combination of three sources:

- The Internet Watch Foundation (IWF) (illegal content)
- The Counter Terrorism Internet Referral Unit (CTIRU) (Prevent)
- 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 associated with prevention of bullying, eating disorders, and child protection.

Monitoring systems[43], are using artificial intelligence in schools to "*continuously build a profile of all users, allowing the system to accurately interpret between a one-off event or a consistent pattern of behaviour.*"

In our research of over 400 schools in England, we are yet to find one policy that makes any mention of the supplier name, or what policy there is on this profiling, keywords of third party access, and retention, error rate, or course of redress. Companies monitor 24/7 every day of the year, including on parent-bought school-use Chromebook purchase schemes, or BYOD bring-your-own-device. Each

---

[40] Safeguarding-in-Schools statutory guidance https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

[41] Working Party 29 Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) p19 http://defenddigitalme.com/wp-content/uploads/2018/05/wp160_en_2009_schools.pdf

[42] NetSupport DNA Education http://www.netsupportdna.com/education/features.asp#safeguarding

[43] Smoothwall Visigo AI Classroom monitoring software https://kb.smoothwall.net/Content/general/Introducing_Visigo.htm

may potentially affect the lives of "half a million students and staff in the UK" or more[44], without oversight or awareness of their accuracy, accountability, or otherwise inside black-box decision-making which is often trusted without openness to human question.

Thanks to Prevent Duty Guidance for England and Wales[45], schools (and registered childcare providers) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Prevent duty guidance expects school staff "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology." In 2015/16 according to the Prevent Programme statistical bulletin[46] 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.

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.*

Child Rights International Network (CRIN) asked schools in London via FOI how they 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 FOI.*" This limits independent scrutiny.

The limitations of filtering technology and over-blocking are clearly set out by Phippen from the 2017 research in, *Invisibly Blighted, The Digital Erosion of Childhood,*[47] 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 to 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. He writes, *"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.'[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. [DfE, 2015] 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."*

The UN Special Rapporteur 2014 report[48] on children's rights and freedom of expression noted: *"The result of vague and broad definitions of harmful information, for example in determining how to set Internet filters, can prevent children from gaining access to information that can support them to make informed choices, including honest, objective and age-appropriate information about issues such as sex education and drug use. This may exacerbate rather than diminish children's vulnerability to risk.*"

Given the length of school hours, and time spent within school property and therefore *in loco parentis* that parents would expect children to spend online without teacher supervision, this technology seems a huge industrial and bureaucratic tool which is disproportionate to its purported aims. The solutions to many of these concerns on child safety are human, not one-size fits all technology. There must be a review of these technologies so that their methods are proportionate, and if harm is to be minimised.

---

[44] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/oral/41158.html

[45] Prevent duty for England and Wales https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

[46] 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

[47] *Invisibly Blighted, The Digital Erosion of Childhood,(2017) r*esearch by Leaton Gray, S. Dr and Phippen, A.Prof. (p92)

[48] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/512/72/PDF/N1451272.pdf?OpenElement

Do you believe children should be able to consent on their own in school to the use of their personal data by third parties (e.g. companies and researchers)?

YES 29%

13% Don't know

NO 58%

Is the current amount of control you have over your child's digital footprint sufficient?

YES 50%

22% Don't know

NO 28%

You said that your school uses Internet Monitoring and keylogging software. Were you offered a choice to use this or not?

YES 54%

NO 46%

Does the Internet Monitoring software used by the school....

Log children's Internet search terms and create flags based on keywords? **55%**

Record screen content as created / seen by the child? **25%**

Record children's image through the webcam? **14%**

DON'T KNOW **28%**

> defenddigitalme believes that parents and children have lost control and oversight of their child's digital footprint in education, even by their fifth birthday.

defenddigitalme.com

Urgent independent review of safeguarding profiling required

1. Web monitoring outside school premises and school hours is not consensual.
   Whether this includes keylogging, screen content or webcam remote access, private space and time must be private, and is beyond the remit of school.

2. Error rates are opaque and system providers have little incentive to be transparent. Teachers concerned enough to contact us said they have children who search for something uncontroversial, the system flags it, and only allows the staff to make a 'note', that it was an error, but not *delete* the error. They were concerned that a move from one system to another created a sudden spike in the volume of flagged words, which all turned out to be baseless. Companies have no incentive to lower their "success rate" of events captured.

3. Security researchers have warned a leading provider of serious flaws in the system design that allow access by third-parties, but the company reportedly failed to fix them.[49]

4. Inaccurate permanent records can be unknowingly assigned to the wrong child. Collecting someone else's web searches and content in-and-outside school hours and assigning the results of monitoring to the child's log-in (i.e. a parent or older brother or classmate prank) could be damaging.

5. Different systems operate different ways with and without school and third party intermediaries. Opaque direct contacts may jeopardise children's trust, where there is,"Proactive Monitoring with unique links to Police.[50] Much more openness is needed of these policies and their implications.

6. Behavioural effects are under researched, but there's qualitative feedback from Leaton-Gray and Phippen (2017) that it has a chilling effect on safe searches for sexuality, health, and teenage development questions.

7. Webcam access for an IT Admin to view the child may mean increased risk of misuse and in potential harm from security flaws. Necessity, proportionality and lawfulness should be assessed.[51]

8. 50% of schools that have responded to us via Freedom of Information requests between December and April 2017 say that they impose this software on personal Bring-Your-Own-Device policies. It is opaque surveillance of personal property, active wherever logged onto the school network.

9. Lack of transparency: parents and children are not informed of the methods and consequences of the web content monitoring and keylogging. 84% of parents in the State of Data survey said they believe they should be informed which keywords get flagged, and 86% want to know what the consequences are — but do not currently know. Where it is felt that this is a Prevent tool for surveillance that is used punitively, there are serious implications for the parent-school-child relationship.

10. Case study: Web Monitoring in unsecured: *"Sites that might be classed as "sensitive personal data" are having the account name and password decrypted. If shop account logons are decrypted then saved credit card data is also accessible. Shops such as M&S and John Lewis, some financial institutions, my doctor's surgery and political parties. This wasn't the case with the county's previous filtering provider. It seems as though they are intercepting every SSL site with the exception of a few manual exceptions. There has been no formal notification of this policy change. Does anybody know on what legal basis County is relying on to intercept these communications?"*

Parents were overwhelmingly in favour of understanding what keywords these systems look for, flag, and what the consequences are for themselves (86%) and for children. (84%)

[49] Security flaw found in school internet monitoring software https://www.theguardian.com/technology/2015/jul/14/security-flaw-found-in-school-internet-monitoring-software

[50] Filtering from Smoothwall https://swgfl.org.uk/products-services/schools-internet-service/filtering/

[51] NetSupportDNA webcam http://defenddigitalme.com/wp-content/uploads/2018/03/NetSupportDNA_webcamgallery.jpeg

Failure to fair process, misleading privacy notices, and consent

There no consistent approach or good standard of national or local setting privacy policy content and approach. There is no good practice to model for apps communication. Some policies include a web link for further information and mention that the school submits data to the national data collections or a link to the DfE national templates and webpage[52], but this requires online access and the proactive work of children or parents, often several clicks and multiple pages away. We have not seen a single privacy policy that explains "we pass your data to commercial companies in X number of apps" or any policy that tells parents and children that their personal data can be given to journalists or commercial companies at national level. Personal data requires fair processing, if it is identifiable or may be identifiable if used with other data that the recipient holds or may be expected to hold.

Privacy notices do not explain profiling or automated decision-making. They poorly explain data collection and may mislead parents by using words like, "*we will not share any of these data without your consent except where the law allows us to do so*."

Schools often include a link to their privacy policy as part of the admissions process. This is lost among as many as 32 multi-page policies parents are expected to read when their child starts a new setting. Policies are not child-friendly. We have seen only one aimed at a child, and that used icons.

In Health there is a strong tradition of confidentiality and clear ethical guidance and an expectation of a consent process before any treatment and intervention. Such explicit traditions are missing in the handling of data in education. The rapid growth of health-related apps used in schools for administrative and special needs, behavioural or "wellness" interventions support, has no oversight or common health and safety assessment. Some collect extended special educational needs, reveal mental health, physical health, and detailed conditions.

medConfidential pointed out to us the importance of conscious use of these apps and technology. "*In an increasingly digital age, trust in institutions requires them to make wise choices for those they serve, to demonstrate that they are trustworthy. All too often, a minor decision, taken for the best of reasons, to help parents or patients, can have entirely predictable adverse consequences that were not considered relevant in advance. Companies get bought, and the best of intentions always die in the face of commercial realities and the endless demands for more data. When the data has gone, whether given, sold, or leaked, it is almost impossible to get it back. Organisations, their tools, and the environments they inhabit can place a label that lasts a lifetime on those they are trying to help."*

Health interventions carried out by the NHS in educational settings are explicitly with parental consent, yet still fail to fairly process the data collected from children at the same time. There is failure to understand at local and regional level in Public Health England or Local Authorities that the National Child Measurement Programme (NCMP) is a named individual level dataset of children's personal data which is passed on to the central databases at NHS digital for indefinite retention. Its linkage with existing or future NCMP data, and other longitudinal health datasets held, or distribution to other third parties are not explained.[53] We have multiple examples of NHS forms used in schools that accompany a consent request (sent home to parents before the vaccination or measurement day) but explicitly and wrongly say, information submitted do not identify individual children.

The National Pupil Database in England

The default position in the UK is for sharing of state-held administrative data for secondary uses, including commercial purposes, as an opt-out, not opt-in mechanism, where one exists at all. For children opt-out is further complicated where parents take decisions on their behalf. There is no opt-out of this database. In December 2015,[54] since its beginnings in 1996, the National Pupil Database contained 19,807,973 individual pupil records on a named basis. Data are retained indefinitely.[55]

[52] December 2017 DfE webpage (accessed March 30, 2018) Data protection: how we share pupil and workforce data https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

[53] National Child Measurement Programme (NCMP) User Access https://digital.nhs.uk/services/national-child-measurement-programme/user-access-controls

[54] FOI request The total number of Unique Pupil Numbers (UPNs) in the NPD as at 28/12/2015 was 19,807,973. This covers pupil records since 2000.

[55] para 3.2.2 pages 31-37. National Pupil Database User Guide v1.3

It is "one of the richest education datasets in the world" according to the Department's own National Pupil Database (NPD) User Guide, a melting pot of over 20 different data collections, census and attainment tests from the Early Years Foundation Stage, Phonics test, Key Stages 1-5, from age 2-19. Each collection is submitted by the school, or setting, generally without parents seeing the data, or any privacy notice. The only notice parents and pupils tend to see, is that during the admissions process.

In our commissioned survey of 1,004 parents[56] 69% say they had never been told their child's data are given away from the National Pupil Database. Families have not been told that sensitive confidential information about individuals from that national database are distributed to others; including for commercial re-use by data analytics firms, by charities and journalists.

National Pupil Database handling must change:

1. All children are vulnerable and their personal data must be safe.
2. Use of all data from the National Pupil Database must be transparent.
3. Every child in education today should be told why their data are being collected.
4. Everyone no longer in school in the NPD who does not know of expanded uses since 2012, must be told.
5. Every researcher should come to the data, stop sending data to them.
6. Every use of data must be made clear to schools that submit it in the census.
7. Stop giving out identifying, sensitive data without consent for secondary, indirect, and commercial uses.

School census instructions sourced from legacy guidance, used across England in 2016 encouraged administrators to ascribe a child's ethnicity, and overrule parents[57], causing outcry in Brighton.[58] Ethnicity is one of only four items in nearly 400 possible entries submitted termly, that parents are able to refuse. However very often parents, after the admission year, are not asked again for data unless there is a new requirement. Parents do not even know it is census day, or get asked to check the data. It is all submitted by the administrator and parents do not check the submission before their own child's named records are sent.

How many may already have been ascribed incorrectly across England since 2000 is unknown. Since the Department for Education (DfE) refuses Subject Access Requests to pupil data in the National Pupil Database, pupils are unable to verify the accuracy of their own data or make corrections.

But millions of children's sensitive personal confidential data at pupil-level have been given away from the National Pupil Database in over 1,000 release to third parties since March 2012.[59] Journalists at national newspapers can get more access to a child's record at national level in England, than their parents or the child themselves.

Third Party Distribution of National Pupil Data

Since 2012, the Secretary of State has had powers to share pupil-level data from the National Pupil Database under terms and conditions with named bodies and third parties who for the *'purpose of promoting the education or well-being of children in England are conducting research or analysis, producing statistics, or providing information, advice or guidance*', and who meet the Approved Persons criteria of the 2009 Prescribed Persons Act, updated in 2012/13.

The data when released however, are not anonymised, but are sensitive and identifying.

"*According to centrally held records at the time of writing, from August 2012 to 20 December 2017, 919 data shares containing sensitive, personal or confidential data at pupil level have been approved for release from the National Pupil Database. For the purpose of this answer, we have assumed the term sensitive, personal or confidential uses of information to be data shares classified as either Tier 1*

---

[56] StateOfData2018 survey: 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

[57] Brighton and Hove CC FOI http://defenddigitalme.com/wp-content/uploads/2016/10/Brighton_Hove_FOI_6956.pdf

[58] Heads in Brighton and Hove were told they could overrule parents who objected and refused ethnicity (the field was since amended to no longer permit this) https://www.independent.co.uk/news/education/education-news/schools-told-to-guess-pupil-ethnicity-a7372271.html

[59] Parliamentary written question - 120141 answered 18 January 2018 Pupils: Personal Records, accessed 2 April, 2018 https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-12-18/120141/

or Tier 2 as set out in the National Pupil Database area on GOV.UK. [In addition] There were 95 data shares approved between March 2012 and this classification system being introduced." [60]

In a presentation to the NPD User group in September 2016, the Director of the DfE Data Modernisation group acknowledged the release of sensitive data: "People are accessing sensitive data, but only to then aggregate. The access to sensitive data is a means to an end to produce the higher level findings."[61]

The data items for release are classed into four tiers by the Department for Education, as described in the NPD User Guide. Following the change of legislation, releases of the data since 2012 from the Department for Education to third parties have not been anonymous, but have been of identifiable and highly sensitive (Tier 1), identifiable and sensitive (Tier 2), aggregated but may be identifying due to small numbers (Tier 3) and identifying non-sensitive items (Tier 4). Raw, closed data are released on a regular basis to third parties, and the majority of releases are of Tier 1 and 2 data.

A list of completed National Pupil Database Third Party Requests and those in the pipeline, are published on a quarterly retrospective basis on the DfE website.[62]

Interdepartmental transfers of data include to the Cabinet Office for preparation of Electoral Registration Transformation work in 2013, to match participant data in the National Citizen Service, and for use in the Troubled Families programme, as well as arms length bodies such as NHS Digital for a survey "What About Youth" mailed home to 300,000 15 year olds in 2014.

The volume of Police and Home Office use first made public through Freedom of Information requests in 2016, were first officially published by the Department, in the Third Party Release Register in December 2017, under "External Organisation Data Shares." We warmly welcomed this new direction of transparency by the Department.

Police requests are only documented in the Third Party Register of External Data Shares going as far back as July 2015. This omits police access to records before this date, as noted in a ministerial correction (HCWS272) made in November 2017 by the Rt Hon Nick Gibb, Minister of State for School Standards, on the numbers of pupils data released to the Home Office and police.[63]

Of the documented requests for identifiable data that have been through the Data Management Advisory Panel (DMAP) request process we believe ca 60% of applications approved (as distinct from volume of data used) were for identifying and sensitive, pupil level data, for use by think tanks, charities, and commercial companies, and 40% by academic institutions (university researchers).

There were 15 rejected applications between March 2012 and September 2016, including a request "by mistake"[64] from the Ministry of Defence to target its messaging for recruitment marketing.

Approved uses include identifying and sensitive data released to Fleet Street papers, "*to pick interesting cases/groups of students,*". The Telegraph newspaper was granted identifying and sensitive data in 2013, for all pupils in the KS2, KS4 and KS5 cohorts for the years 2008-2012.
An FOI request at whatdotheyknow.com Ref: 2015-0054037 confirmed that the release of 5 years worth of data to the journalists, at pupil level, was without suppression of small numbers, and included children's sensitive personal data including SEN and FSM indicators, ethnicity and language. These identifying and sensitive items, or identifying data items were matched at individual pupil level with school census data for Key Stage 2, KS4 and KS5 datasets before release at individual level.[65]
There is little detail on the precise use of the data. We were able to get access to the original application form, but were told that, "*There is no further written business case for the approved Tier 2*

---

[60] Written parliamentary question 120141 January 2018 https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-12-18/120141/

[61] Presentation to the NPD Bristol User Group 2016 http://www.bris.ac.uk/media-library/sites/cmpo/documents/bradley2016.pdf

[62] External data shares https://www.gov.uk/government/publications/dfe-external-data-shares

[63] Correction:Written statement - HCWS272 In response to PQ48634 and PQ48635, the correct figures are that 33 access requests of the NPD data were made by the Police during the period in question and 16 of these resulted in data being shared. Information about 62 pupils was shared. https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2017-11-27/HCWS272/

[64] Schools Week MoD requests sensitive pupil data by mistake https://schoolsweek.co.uk/mod-makes-inappropriate-request-by-mistake/

[65] The Telegraph promise not to *publish* children's identifying data http://defenddigitalme.com/wp-content/uploads/2018/03/telegraph_email_snap.jpeg

variables other than what is included in the application form. After a telephone discussion with the Daily Telegraph, the Tier 2 variables requested were subsequently approved as they were required to differentiate between the different intakes that schools have. To effectively compare schools, the Daily Telegraph wished to factor in the "different types of pupil" who are present at different schools. Information on pupil characteristics related to prior attainment: gender, ethnic group, language group, FSM eligibility and SEN provision status were deemed by the Department to be appropriate as these are seen as important factors in levels of pupil attainment. The approved Ethnic Group Major and Language Group Major variables are the least sensitive versions available of this data.

"At the time of this request (Feb 2013) we did not require the requestor to inform us of the conditions for processing that they relied on. The requestor signs an agreement which confirms that they will process the data in accordance with the Data Protection Act (DPA) and it is the responsibility of the requestor to ensure this is the case. As such there is no written evidence available of the condition for processing under Schedule 3 of the Data Protection Act that the Daily Telegraph relied on."

The raw data are sent to the requestor's own location. DfE does not charge for data (and has not since the NPD process began), nor does DfE charge for the processing and delivery of extracts to customers.

There is no transparency of the volume of how many children's data have been given away in each of the over 1,000 approved uses, because,"*the Department does not maintain records of the number of children included in historic data extracts.*" (PQ109065)[66] According to our analysis of national pupil data releases between 2012 and May 2017, 28% of the approved 1,000 releases were for commercial use. Adding think tanks and charities, it becomes closer to 60%, leaving only 40% for what the public might consider bona fide "public interest" research.[67]

Public interest research use of pupil level data may also be through other routes of access to the data, comparatively safer routes using safe settings, and may include projects linking individual data together with other education and employment data from citizens' interactions with other government departments and public services. For example, the LEO dataset is made up of information from the National Pupil Database (NPD), the Individualised Learner Record (ILR), the Higher Education Statistics Agency (HESA), Her Majesty's Revenue and Customs data (HMRC), The National Benefit Database, the Labour Market System and Juvos, the unemployment research database. Further work by DfE compares self-reported salaries from the 2008/09 DLHE survey with earnings data from the LEO (Longitudinal Education Outcomes) dataset coming directly from HMRC records.

New data analytics products and services have been developed using taxpayer funded data created and collected in schools. Time is spent on cleaning and distribution, before it is given away to for-profit companies that process the data into analytics and benchmarking products[68]. Schools and Local Authorities then buy in the processed data, for use as 'accountability measures'. School census data are sent every term, plus attainment and come to over 50 submissions in a child's lifetime education. Does the cost-benefit analysis justify this burden, and does privacy factor into the intangible costs?

What are "research purposes" and where do we draw the line with commercial exploitation? Think Tanks? Private tutor companies? Journalists? Data are being used in predictive modelling for exclusion, linked with Police National Computer data, and used by a renowned research Institute of Criminology. What risks do any inaccuracies and profiling communities of like-characteristics pose?

Schools process data about criminal offences, exchanging information with YOMS and police. But many more read similarly, and yet has not been any conviction; in reasons for exclusion such as theft, violence, and other misconduct. However these data are not treated with the same retention periods as the Rehabilitation of Offenders Act 1974 but are retained indefinitely, and at national level may be distributed to a wide range of third parties at pupil level, long after the child has left school.

Parents and pupils themselves are not sufficiently aware of the way the data is being shared with third parties, and there appears to have been no plan to bring these third-party uses of their personal data to the attention of parents or pupils. Our survey found that while parents give the Department for Education a high level of trust to use data well (68%), almost the same number of parents (69%) said they had not been informed the DfE gives out data from the National Pupil Database to third parties.

---

[66] PQ109065 Pupils: Personal Records October 2017 https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-10-23/109065/

[67] Analysis of national pupil data use approved applications (volume of data sent unknown) http://defenddigitalme.com/wp-content/uploads/2017/04/chart.jpg

[68] Sample benchmarking product by a third party using data from national pupil data https://i0.wp.com/defenddigitalme.com/wp-content/uploads/2018/05/FFT_clip.jpg

Children's data rights are ignored for the National Pupil Database

- No Subject Access Rights [PQ 108573][69]
- No Right to Rectification
- No Right to Erasure
- No Right to Object to Processing
- No Right to Restriction of Processing

Schools did not inform ex-pupils of the change of DfE national data uses since the legislation changes in 2012 and neither did the Department. Since legislation changed over time to permit new uses and access to personal data by new third parties, over 15 million people whose data was already in the National Pupil Database and who had already left school pre-2012, have not been informed how their personal data may be used, and by whom.

But just like DotEveryone[70] recent work found on digital attitudes, our poll found that the public want to know how their personal data are used. Over three quarters (79%) said if offered the opportunity to view their child's named record in the National Pupil Database, they would choose to see it.

Recommendations on National Pupil Data rights

1. Parents and pupils should be empowered to understand where their data has gone, and understand its benefits — in public interest research — as well as the risks. This must include everyone in the database — pupils presently in school, and those who have left.
2. Restore and respect child rights in data privacy and protection. The DfE should restore Subject Access Rights for children to be able to see their own records. [PQ 108573]
3. Communications with pupils and parents need to be consistent across the sector. Schools have no way to tell families who has copies of their child's data through access to both local and national level data and linkage, such as Fischer Family Trust, the Education Endowment Foundation, RM and anyone else who holds copies of the entire national pupil database.
4. The GDPR recognises that children merit specific protection, so any information and communication, where processing is addressed to a child, should be in clear and plain language that the child can easily understand. This shift demands a change of wording and change of policy and practice to meaningfully inform children and parents how and why data are used compared with today, where privacy policies fail.
5. At national level, data need to be documented which data in which databases come from which sources, if children and parents are to have a hope of later oversight not only with third parties receive national data, but which third parties received *their* individual personal data in particular. A longer term transparency tool for individuals, might be in the form of data usage reports, to be able to see what data are held, where data have gone and its uses, which may differ since explained on collection, or be unexpected if ascribed.
6. Retention and distribution policies need review at all levels, starting with sensitive data and exclusion data.

National Pupil Data are a cumulation of various collections of local pupil data, few of which were originally collected form parents / guardians during the admissions process or course of a child's education. Much more is created by school staff, through transfers of data from other schools in Common Transfer Files and other notes, or comment, opinion, and ascriptions from various staff.

Formal attainment data are provided by schools in results' submissions but also from awarding bodies to the national pupil database. These multiple sources may mean that errors in personal data at national level, are almost impossible for an individual to trace unless the source trail is documented. For now, this is not available in the public domain.

School-wide seamless integration with the pupil information management systems, mean for both national and local systems, the distribution of data is much easier than keeping track of where it went. Children's personal data are sent to a range of commercial third party providers to create accounts *before* the parent and pupil have been informed if they are ever informed, without any choice or ability

[69] Pupils: Personal Records:Written question - 108573 October 26, 2017 https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-10-18/108573/

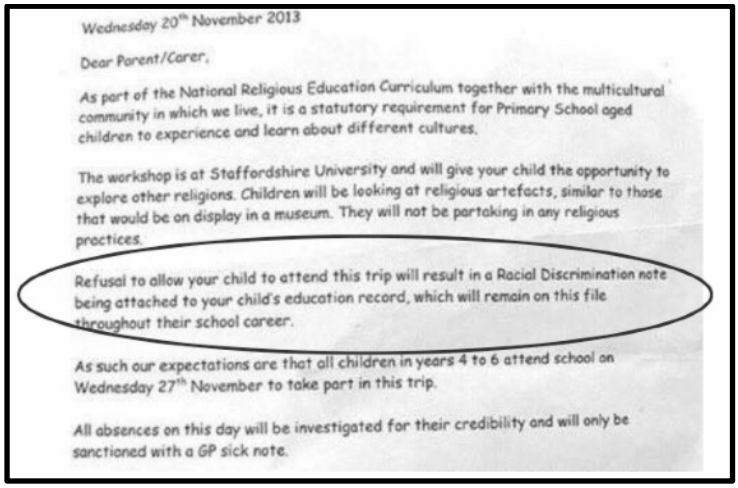
[70] Miller C, Coldicutt R and Kitcher H. (2018) People, Power and Technology: The 2018 Digital Attitudes Report. London: Doteveryone. http://attitudes.doteveryone.org.uk/

to say no where the school makes a choice to use an app or third party provider and where the department for education hands it out to research organisations in bulk from the national databases. Structuring this audit trail in a manageable way may be a task best suited to today's systems integrators at local level, but must happen at national level as well, where there is onward sharing.

Data retention is an issue coming of age with maturing local systems, and indefinite retention at national level. Names once collected for research linkage, are now being used for research mailshots[71], direct interventions that can cause harm and distress in immigration enforcement, and for predictive modelling and interventions. "*Because children are developing, the data relating to them change, and can quickly become outdated and irrelevant to the original purpose of collection*" the WP29 in 2009 recommended, "*data should not be kept after this happens*." [72] Review of retention and ongoing uses, merit urgent attention and action.

Where is the harm? A glimpse into how things go wrong

Poor practice can be systemic and supported by poor technology design or legacy ascription fields. It can also be unique to a school's own policy and practice. For every child however, anything which is attached to their record "throughout their school career" and sent to national pupil databases, now means labelled for life. These decisions are not always given due thought and could have severe unintended consequences.



Wednesday 20th November 2013

Dear Parent/Carer,

As part of the National Religious Education Curriculum together with the multicultural community in which we live, it is a statutory requirement for Primary School aged children to experience and learn about different cultures.

The workshop is at Staffordshire University and will give your child the opportunity to explore other religions. Children will be looking at religious artefacts, similar to those that would be on display in a museum. They will not be partaking in any religious practices.

Refusal to allow your child to attend this trip will result in a Racial Discrimination note being attached to your child's education record, which will remain on this file throughout their school career.

As such our expectations are that all children in years 4 to 6 attend school on Wednesday 27th November to take part in this trip.

All absences on this day will be investigated for their credibility and will only be sanctioned with a GP sick note.

Data errors

There has never been any data audit of England's National Pupil Data released in the public domain. How can errors be identified or corrected? By comparison in Wales, the government permits subject access requests. In the 2017-18 school census Welsh Government guidance pointed out that the default setting for a school information management system field, and therefore school census data, was wrongly coded — it indicated by default, that every child had in the past been a Looked After Child. This was only identified when a parent made a Subject Access Request about their child which the Welsh government fulfilled, revealing that every child in 2010 had been wrongly recorded as having been in-care at some point in the past. Scotland and England do not permit Subject Access Requests.[73]

> Our wider investigation has revealed that in 2010 the software used by schools in Isle of Anglesey incorrectly used the code 'XXX' as the default value for this field, leading to all pupils having this code whether they were in care or not. Our validation rules for this field

Data misuse

A former council worker in the schools admissions department of Southwark Council was fined for sharing personal information about schoolchildren and parents via Snapchat.[74] The defendant took a screenshot of a council spreadsheet concerning children and their eligibility for free school meals before sending it to the estranged parent of one of the pupils. The image included the names, addresses, dates of birth and National Insurance numbers of 37 pupils and their parents.

---

[71] i.e What About YOUth? Survey 2014 http://defenddigitalme.com/wp-content/uploads/2018/05/what-about-youth-eng-2014-rep.pdf

[72] Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) http://defenddigitalme.com/wp-content/uploads/2018/05/wp160_en_2009_schools.pdf [page

[73] Our comparison of UK National Pupil Databases http://defenddigitalme.com/wp-content/uploads/2018/05/UK_pupil_data_comparison_May2018.pdf

[74] ICO blog, Former council worker fined for sharing personal information about schoolchildren and parents via Snapchat, 22 February 2018, [accessed 1 March 2018] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/02/former-council-worker-fined-for-sharing-personal-information/

1996 Section 537A of the Education Act 1996 governs the principles for the provision of information about individual pupils.

Successive secondary legislation expanded the personal data about individual children that are collected and linked in the melting pot of the National Pupil Database

1998

Education (School Performance Information) (England) Regulations 1998, 1998/1929 (made under sub-s (1)).

Education (Individual Performance Information) (Identification of Individual Pupils) Regulations 1998, SI 1998/1834 (made under sub-s (2)).

1999

The Education (School Performance Information) (England) Regulations 1999

2007

Education (Information About Children in Alternative Provision) (England) Regulations 2007, SI 2007/1065.

Education (School Performance Information) (England) Regulations 2007, SI 2007/2324.

Education (Pupil Referral Units) (Application of Enactments) (England) Regulations 2007, SI 2007/2979.

2008

Education (School Performance Information) (England) (Amendment) Regulations 2008, SI 2008/364.

Education (School Performance Information) (England) (Amendment) (No 2) Regulations 2008, SI 2008/1727.

Special Educational Needs (Information) Act 2008 http://www.legislation.gov.uk/ukpga/2008/11/contents

2009

Education (Individual Pupil Information) (Prescribed Persons) (England) Regulations 2009, SI 2009/1563 (made under sub-ss (4)–(6)).

Education (School Performance Information) (England) (Amendment) Regulations 2009, SI 2009/646.

2010

Education (Individual Pupil Information) (Prescribed Persons) (England) (Amendment) Regulations 2010, SI 2010/1940 (made under sub-ss (4)–(6)).

2012

Education (School Performance Information) (England) (Amendment) Regulations 2012, SI 2012/1274 (made under sub-ss (1), (2)).

2013

Education (Individual Pupil Information) (Prescribed Persons) (England) (Amendment) Regulations 2013, SI 2013/1193 (made under sub-ss (4)–(6)).

Education (School Performance Information) (England) (Amendment) Regulations 2013, SI 2013/1759 (made under sub-ss (1), (2)).

Education (Information) (Miscellaneous Amendments) (England) Regulations 2015, SI 2015/902.

2015

Education (School Performance Information) (England) (Amendment) Regulations 2015, SI 2015/1566.

Small Business, Enterprise and Employment Act 2015 (whcih enabled linkage of NPD, HE, FE with datasets to create the "destinations data" and LEO)

Education (Pupil Information and School Performance Information) (Miscellaneous Amendments) (England) Regulations 2013, SI 2013/3212.

Education (Pupil Information) (England) (Miscellaneous Amendments) Regulations 2016, SI 2016/808 (made under sub-ss (1), (2)).

2016

2017

The Education (Information About Children in Alternative Provision) (England) (Amendment) Regulations 2017 SI 2017/807.

1996 "such individual pupil information as may be prescribed"

For Key Stage one, two and three, GCSE, GNVQ and A level pupils age 5-18. School information, name, address and telephone number of the school. Number of pupils on roll including breakdown of number with Special Educational Needs.

1998

Legislation enables collection of pupil-level data in 1996. Secondary legislation starts this expansion in 1998 to date of birth, gender, surname, first names; the level of the National Curriculum scale achieved, working below level, not achieved, or not taken. Named start 2002.

1999

Alternative Provision children's surname, first name, date of birth; address and postcode; unique pupil number, gender; special educational needs provision (SEND); ethnicity; whether English is not the first language; whether eligible for free school meals; and ype of funded provision attended, that is whether it is a hospital (other than in a school established in a hospital); independent school; or a hospital or school.

2007

Admission date, ethnicity, first language, home address and postcode, Free School Meals (FSM), Looked After Child (LAC), Special Educational Needs (SEND) , Key Stage Results, reasons for authorised and unauthorised absences. Provision of Information to the National Data Collection Agency and the External Marking Agency.

2008

Broadened information about children with special educational needs and their well-being.

SEND types are one of 13 codes for type of learning difficulty, moderate , profound, multiple, specific. Social, emotional and mental health, speech, communication and language needs, hearing, multi-sensory or visual impairment, physical disability, autistic spectrum disorder, other difficulty, SEND support but no specialist assessment.

Each approved external qualification taken by the pupil at Key Stage 4 and the grade or, where applicable, the level achieved.

2009

Legislation broadened out to which specified prescribed persons government can give individual level data.

2010

Legislation broadened the purposes for which data could be shared with the specified prescribed persons who, for the purpose of promoting the education or well-being of children in England are conducting research or analysis, producing statistics, or providing information, advice or guidance.

Phonics screening check results, Assessment and reporting arrangements Year 1 whether the pupil attempted to read the word, and if so, whether the pupil read the word correctly or incorrectly. Gender, date of birth, surname, first names;, unique pupil number.

2012

2013

For children in Pupil Referral Units, unique pupil number and learner number, gender, date of birth, surname, first names; ethnicity, first language, National Curriculum Year Group. Looked-after child and LAC authority name, adoption order, residence or guardian order, Where child is excluded, the reason for the exclusion, type of exclusion (fixed period or permanent). Removal of the requirement to provide pupil's usual mode of travel to school, ethnicity source (ascription), Gifted and Talented cohort.

SEND primary and secondary need of those types if there is more than one type. Whether statement or an Education, Health and Care plan in place.

2014

2015

Small Business, Enterprise and Employment Act 2015 (Destinations data for linkage of all of this data with longitudintal educational outcomes - the LEO dataset)

Country-of-birth, nationality, proficiency in speaking, reading and writing in English. Age of collection of ethnicity reduced in practice to age 2+.

2016

Information About Children in Alternative Provision: date of entry, leaving frequency of attendance, individual special educational needs, primary reason for funded provision placement

2017

Reason for placement is one of eight: Other, Setting named on Education Health and Care plan, Mental health need, New arrival without school place, Pregnancy / Childcare, Physical health need, Young Offender institute / Secure unit, Permanent exclusion,.

These are the core personal data of the ever-growing National Pupil Database, a melting pot of data from now over 23 million people.

Acknowledgements

Hundreds of individuals across the education, data privacy and data protection sectors are helping us map the sector and some of its key issues as merit attention for legislative or policy improvements. Civil Society, Civil Liberties and Child Rights advocates and organisations have supported our own better understanding. Thank you to each one. Written comments or FOI have been included from:

Biometrics-in-Schools

Pippa King is a parent whose children were nearly fingerprinted in 2005 without her consent when they were 6 and 7 years old for a school library system. She was shocked to be told that the school did not need to ask her permission to take her children's fingerprints.The Protection of Freedoms Act was passed in May 2012 which requires, in chapter 2 clauses 26-28, for schools to gain written parental consent if they wish to store/process a child's biometric data. Pippa is a leading expert in biometrics technology and continues to campaign for children and parents' rights. She is also a Director of defenddigitalme |
Info: http://pippaking.blogspot.co.uk/p/home.html | Email: biometricsinschools@gmail.com

Child Rights International Network (CRIN)

Child Rights International Network - CRIN is company limited by guarantee number 06653398.
Info: https://www.crin.org/ | Email info@crin.org

Liberty

The Civil Liberties Trust, is a registered charity in England and Wales (No. 1024948) that exists to support the work of Liberty. The National Council for Civil Liberties is a company limited by guarantee registered in England and Wales number 3260840.|
Info: https://www.libertyhumanrights.org.uk/ | Contact tel: (+44) 20 7403 3888.

medConfidential

medConfidential campaign for confidentiality and consent in health and social care and work to ensure every flow of data into, across and out of the NHS and care system is consensual, safe and transparent. medConfidential is a company limited by guarantee with charitable objects number 08495396 |
Info: https://medconfidential.org/ | Contact: coordinator@medconfidential.org

Rights Watch (UK)

Rights Watch (UK) work to promote just and accountable security by ensuring that the measures taken by the UK Government in pursuit of national security are compliant with human rights and international law. Rights Watch (UK) is a registered charity 1048335 and company limited by liability no. 2489161| Info: http://www.rwuk.org/ | Contact tel: (+44) 0203 6030 972 | Email: info@rwuk.org

and with thanks to

EduGeek

The IT staff survey views was made possible only through the support and cooperation of EduGeek volunteer staff who generously reviewed and edited the questions to be suitable for their colleagues. We must also thank the other forum participants whose ongoing comments and questions continue to prove to be an invaluable resource to deepen our knowledge of applied practices, questions and issues. http://www.edugeek.net/

Further comments from IT staff on GDPR readiness at 35 UK schools http://defenddigitalme.com/wp-content/uploads/2018/03/Staff-views-on-GDPR-readiness-in-schoolsv5.pdf

We are also enormously grateful to the Joseph Rowntree Reform Trust Ltd. for continued support enabling our work throughout 2017-18 and to the Lush Charity Pot for financial support towards the print and distribution costs of the draft interim report to policy makers in May 2018.

You said your school uses biometric technology. Were you offered a choice whether to use this system or not?

NO 38%

defendigitalme believes a Code of Practice is needed that covers use of children's biometrics and better data protection practice. The 2012 Protection of Freedoms Act requires both parents and the child to be asked for consent to use a child's biometrics, and an alternative method to be on offer. .

Were you informed of how long the fingerprint, retinal scan, palm scan or facial image recognition data are kept by either the school or the company that provides the service?

NO 50%

It is a basic Principle of data protection law today, to communicate well with the people whose personal data that are being processed, for processing to be fair and lawful. That includes how long you plan to hold data for and to ensure that retention periods are respected. This is a key issue for maturing school systems and the rights and responsibilities of parents and schools today.