Defend Digital Me edTech and pupil data Briefing: November 2023

To reduce the debate on edTech to questions of data processing or particular pros and cons of a single product is to misunderstand the socio-political and economic underpinning and goals of the edTech market.

Fundamentally the introduction of many common technology tools, apps and platforms into the school setting means the introduction of hundreds, often thousands of strangers who influence a child's life through interactions with companies and their affiliates in the digital world.

Data analytics by an edTech product directly is often just the start of a chain of third parties that can peer over a child's shoulder and profile everything they do whether through the adTech ecosystem, through the redistribution if not always selling of personal data for commercial analytics or packaged as a research resource. The relentless surveillance of the learner's activity and behaviours, from log on time, length of time spent using the product to mouse clicks and profiling mean the datafied child has become a valuable by-product of a system intended to support their right to education and flourishing into adulthood. But it is without oversight of company objectives, tone, language, pedagogy, methods of punishment or praise that could affect a child's development or even be designed to nudge their mental health, all in ways that a parent, or indeed the teacher cannot see beyond company marketing. If I send my child to school in England in 2023 who will be allowed to influence their development? What does that mean for their digital footprint and digital identity for life? What does outsourcing the delivery of now crucial parts of the state education system to commercial actors mean for the future control, delivery, costs, stability and sustainability of UK state education? And are the incentives and aims of education aligned across all those involved –if profit motives conflict with the bests interests of a child or the duty of care by an educational setting, or a product causes harm through discrimination or redirecting a child's learning or future career interests in ways that cannot be seen by edTech that claims to "steer" children's mental health, who and how can parents hold staff or companies accountable?

Our own research of applied edTech in schools in England supports the conclusions reached by academics at Edinburgh University, "The range of investors in EdTech includes venture capital, private equity and strategic investors. EdTech-specific investors are political actors that construct, promote and operationalise particular ideas of education and its future. Second, investors increasingly finance products and platforms that bypass the gatekeepers within the school system to deliver EdTech directly to young people, their families and lifelong learners." [1]

> "edtech investors require further research attention because they are responsible for reshaping #education by structuring the #edtech industry".[2]

What that environment looks like may be unfamiliar if you did not use it when at school. It is not a single homogeneous place. The provision of physical infrastructure is controlled by different companies and often it is not owned by the educational setting at all. Other people's computers, cloud-based data storage companies, may each store thousands of schools' information management systems and hand over millions of pupil records every minute to other apps and virtual learning environments that school staff decide to use, signing up pupils and often parents personal detail originally provided to enrol the child at school, to an unlimited number of outside companies .A child is signed up routinely to a dozen by the setting before the child has left primary school.

[1] Davies et al. (2023) Investigating the financial power brokers behind EdTech https://educationdatafutures.digitalfuturescommission.org.uk/essays/competing-interests-in-education-data/investigation-financial-power-brokers-edtech

[2] https://codeactsineducation.wordpress.com/2023/11/03/the-power-of-edtech-investors-in-education/

Hardware used might be mobile phones, Chromebooks, iPads owned by schools or privately by families, or third-party company servers with access for the local authority, police, research or national databases (defenddigitalme, 2020). What the digital environment looks like from a family's point of view is increasingly intrusive into private and family life, with more and more companies accessing or monitoring pupils' personal devices including web cameras, and more and more use cases made for processing a child's biometrics or bodily data in 'trait and gait analysis' (defenddigitalme, 2022) The information highways, the roads on which data flows across the digital landscape, the vehicles transporting it around, the browser windows of how people in it can access information, the places information is stored and who has legal jurisdiction and police authority and the owners of every part of the landscape may each be different and each have hundreds of affiliate 'internal' companies.

In summary, edTech should not be thought of as a technology product problem, or all about data protection. We must consider how these issues play a part in holistic approaches to the delivery of state education framed within our position in an international landscape and the aims of education, as set out in both conventions and laws, supported by strategies to further the rights of the child.[3]

Open questions around edTech in educational settings

1. **Does adequate evidence exist for the educational outcomes, social development and protection of children's rights in edTech in England?**

   No. Across the UK, there is very limited independent evidence of the outcomes for children using edTech in routine learning apps and platforms, little on imposed device SafetyTech, and even less on claims made by companies or their trustworthiness and integrity providing schools with emerging technology already in or being trialled in UK schools such as Artificial Intelligence, mood and emotion scanning[4], AR and VR or haptics in wearables, sport wristbands in schools[5], robots used in social reading support or neurotechnology[6] such as brain scanning headbands[7].

   In England evidence of edTech trial[8]s (see later comments on product development and commercial research ethics practices) has been commissioned by the DfE at the EFF "(The Department for Education (DfE) has confirmed its re-endowment of the Education Endowment Foundation (EEF) with a grant of £137m to put it on a long-term footing and continue its work as an independent evidence broker, evaluating and spreading best practice across English schools, nurseries and colleges, for at least another decade". However a significant number find no evidence of benefit or even find harm. In one case study a

[3] Council of Europe Strategy for the Rights of the Child 2022-27
https://rm.coe.int/council-of-europe-strategy-for-the-rights-of-the-child-2022-2027-child/1680a5ef27
[4] This technology was trailed in a school in Wolverhampton
https://www.intel.com/content/www/us/en/developer/articles/technical/viewsonic-displays-for-the-smart-classroom.html
[5] In this trial "Some school staff also reported concerns over wearables impact on student mental health and well-being (e.g., obsessive tracking behaviours)." https://www.mdpi.com/1660-4601/19/21/14067
[6] "Pearson has itself articulated a vision of AI teaching assistants and cognitive tutors using technologies based on advances in educational neuroscience and psychology. "
https://codeactsineducation.wordpress.com/2017/05/04/brain-data-neurotechnology-and-education/
[7] https://qz.com/1742279/a-mind-reading-headband-is-facing-backlash-in-china
[8] EEF trials https://educationendowmentfoundation.org.uk/projects-and-evaluation/projects

product that we at Defend Digital Me researched in depth including obtaining original correspondence from Australia about the biometric data collection,found, "pupils in schools that received Visible Learning, made, on average, one month ***less*** progress in combined KS2 maths and reading compared to children in the control schools"[9].

The DfE in Westminster, has a ten year-old voluntary self-certification for cloud based apps. and publishes a selection on the DfE website.[10] Some of the larger providers complete this however none ever find anything unlawful, unethical or unsafe in their practices. We suggest many of these are not entirely accurate or complete findings.

In 2023 new 'standards'[11] have been published by the DfE focussed on cyber security or 'infrastructure' type issues such as broadband, but to the best of our knowledge, these are voluntary in the spirit of advice and guidance and are not technical standards underpinned by an audit or accountability regime for England.

There are no enforceable standards on educational outcomes, pedagogy, permitted interventions or advertising and marking in edTech products, or restrictions on technology that is found to make misleading claims, that simply does not work, or affects children's development behaviour, mental health, or social attitudes– while the Scottish Local Authorities[12] have a role in vetting edTech before it may be procured in schools in Scotland, and in Wales the government may make interventions such as to make Google Classroom compulsory overriding any parental objections in 2020, no such authority exists in England.

edTech is rolled out without quality, health and safety standards, inspection or routes for complaint or redress; the latter made especially difficult when the school is in a position of authority and a non-consensual environment which parents are loathed to upset given the importance of school-home relationships for a child.

2. **Data processing lacking a lawful basis:** Consent is not a valid basis for data processing for routine required educational practice due to the power imbalance between the authorities and child/family (as seen in regulatory and legal precedents in Sweden and France on the use of facial recognition that claimed to operate on the basis of consent) which impairs its freely given nature, and yet it is often "assumed" or simply not given due thought when schools sign children up to apps without asking them, often not even informing parents first.

   "Public Task Article 6(1)(a) or 8(1), "*for the performance of a task carried out in the public interest,*" is the data protection ground for most data processing done by an educational setting. This carries the obligation to offer a right to object. This is rarely offered or

[9] https://educationendowmentfoundation.org.uk/projects-and-evaluation/projects/the-visible-classroom-2015

[10] While this covers some providers it is a tiny sample of tools in practice and the standards are 'suggested guidance' not requirements or technical standards to which any educational institution is held accountable or audited https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644845/Cloud-services-software-31.pdf

[11] DfE (2023) Meeting digital and technology standards in schools and colleges https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/broadband-internet-standards-for-schools-and-colleges

[12] Scotland FOI example of Dundee's approved and rejected edtech apps (2019) https://www.whatdotheyknow.com/request/edtech_provider_approvals_proces_5

respected in schools and poorly understood.[13] The 2020 ICO audit[14] of the Department for Education found that," there is an **over reliance on using public task** as the lawful basis for sharing which is not always appropriate and supported by identified legislation. Legitimate interest has also been used as a lawful basis in some applications however there is **limited understanding of the requirements of legitimate interest** and to assess the application and legalities of it prior to sharing taking place how it should be applied to ensure the use of this lawful basis is appropriate and considers the requirements set out in Article 6(1)(f) of the GDPR."

3. There is little consistent effort made to address **what "*data protection by design and default*" in practice means, or [child] appropriate 'significant legal effect**' (Baroness Ludford, Second Reading, House of Lords debate on the Data Protection Bill 2017 Col 144-5). The redefinitions of personal data and research in the Data Protection and Digital Information Bill (2023) will affect children in schools as anywhere else.

4. **Security**: EdTech introduces new risks at scale into schools. In 2017 US-based education platform Edmodo confirmed 77 million account details were stolen – more than 2 million of them in the UK – across 550,000 schools worldwide. If a pupil or parent cannot object to using an app for maths homework, parent-school communications, or sickness reporting and yet it poses the child an unwarranted risk to their identity, security or that of family members how can parents ensure their safety? Does an obligation to deliver education include any software use is compulsory, rather than the aim behind it?

5. **"Research"** has come to be defined as anything can be imposed by any outside party the school deems fit but without necessarily research standards, ethics or evidence of efficacy – this is important with regards to AI and the new DPDI Bill which seeks to do this for all personal data – redefining research also redefines when research exemptions apply to personal data. Should children or families be able to object to being part of edTech trials, interventions, and their resulting datafication and loss of control of personal data?

6. **Respect and routes for exercising rights:** Both parental and child rights as well as institutional obligations, need taken into account (UDHR Article 26 (3)(b)
    a. Why is the Right to Object not offered when it is a necessary part of the data processing rules around the lawful basis most often used in educational settings: public task? If an EdTech is introduced the aims or ownership or data processing of which a parent disagrees, should parents not be able to exercise the right to object just as they can for participation in school assemblies for reasons of philosophical

[13] See the Right2Object project at Winchester University by Dr Caroline Stockman (Department of Education Studies and Liberal Arts), Dr Emma Nottingham (Centre for Information Rights) and Prof. Maria Burke (Head of Research and Knowledge Exchange, Faculty of Business, Law and Digital Technologies).
https://www.winchester.ac.uk/about-us/leadership-and-governance/our-faculties/lcj/centre-for-information-rights/right2object-project/

[14] ICO DfE audit executive summary (the full 139 recommendations has never been published, refused under FOI)
https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf

beliefs? Whose values are permitted with what oversight to influence my child in loco parentis? If an edtech or product trial has caused harm, what is the redress?

b. Where are the responsibilities between a company and school for 24/7 surveillance of activity using the school server? What about edTech used in homework? And are families simply allowed to email staff 24/7 365 days a year and complain if they think the reply is not fast enough? Boundaries between home and school geographically and in time, term time and holidays, have been lost.

7. **Staff training**: Latest research from SWGfL(South West Grid for Learning) on online safety provision, has found that over one third of schools across England lack effective staff training despite this being a statutory requirement for schools, and school governors. The same question is not even asked of edTech or data literacy more broadly.

8. **Advertising exposure:** The DfE has a [self-certification scheme for cloud providers] albeit, a decade old. Despite recognising (page 8) that children may not be competent to understand how their personal data is used in adTech there is no guide if or how this should be done:

> "t*here are obvious difficulties with schools deciding if children are competent enough to understand any explanation of their data being used for advertising, and to understand and exercise their right to object, without parental involvement,*"

In research of over 300 privacy and edTech policiesDefend Digital Me is yet to see any that is a role model of good practice for parental involvement.

Case studies: EdTech and data processing in the state education system in England

Background summary

Technology is used to collect the statutory pupil data returns across 23 termly/annual collections for the 9 million in education today, that is collated together by the Department for Education into the National Pupil Database, now holding ca. 28 million individuals named records, to which named equality monitoring data (religious affiliation, sexual orientation, disability) are added and retained on a named basis from Higher Education. There have been over 20 statutory instruments since 1996 that have expanded the UK government's data collection and processing powers of pupil data in England, but none expanded any safeguards. Since 2012, every learner's personal data in the National Pupil Database has been opened up to give away to businesses and other third parties after the government changed the law to create a market for the re-use of pupils' records.[15]

Together with the rapid expansion of educational technology in the UK exacerbated under Covid-19 to support distance learning, and the wide variety of apps and platforms used across a typical secondary school pupil's day-in-the-life (Fig.1), this means thousands of companies process millions of children's highly sensitive and identifying data obtained indirectly from school systems, or from children's direct interactions, 24/7, 365 days a year, out-of-school-hours and beyond school gates.

[15] Defend Digital Me: A Timeline
https://defenddigitalme.org/national-pupil-data-the-ico-audit-and-our-work-for-change-a-timeline/

.

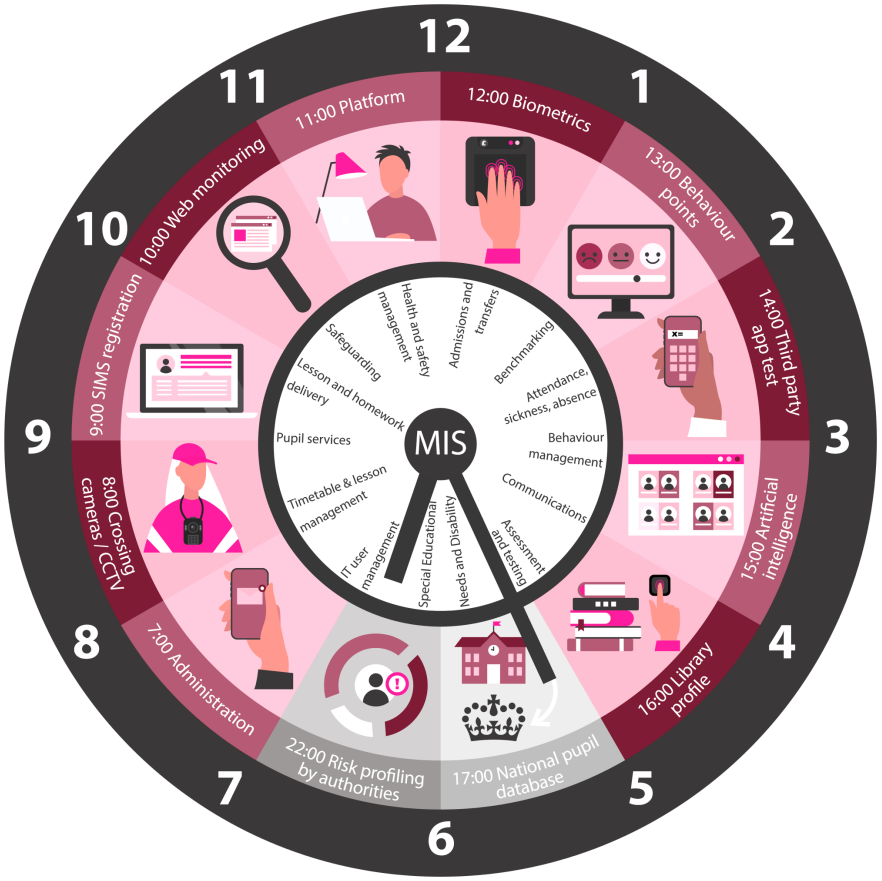

Fig.1.

School staff recognise that they want extra help and support

In 2017, evidence from 4,507 of 6,950 schools using the SWGfL tools who carried out e-safety self-reviews, using the 360 Degree Safe tool in analysis carried out by Professor Andy Phippen at Plymouth University[16] shows that school staff are not equipped to deal with or challenge the outcomes from these technologies..

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

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

In 2018, Defend Digital Me carried out a small sample of schools policies via ICT staff. The full findings can be viewed here[17]. But in summary **94% had no communication policy today for school leavers to tell them how their personal data will be retained,** its legal storage requirements and retention periods or when it will be destroyed is not explained. (eg. if or when data will be deleted from apps used in learning platform providers, from school records, or by other third-parties).

Only 1 in 5 had communicated a **Subject Access** policy to pupils and parents.

Only half (49%) agreed they had **informed processing** and were able to tell a child or parent today where all their personal data goes when it leaves school. (For example, used in third party apps., pupil data systems, census, LA or MAT etc. Ofsted, or in research).

Under 20% in England tells parents/pupils explicitly which organisations may use identifying personal data submitted to the Department for Education in the termly or annual school census. 23% say they do not inform pupils and parents what the Department for Education does with pupil data, and **an additional 23% said they were not themselves aware** of individual-level pupil data third-party distribution of national pupil data.

When asked **how pupil level data can be accessed**. 60% said that all staff can access all data across the school information management system. In 43% school staff use their own personal phones, hand-held devices, or laptops to access pupil level data; and in 34% of those schools who responded, there is use of USB sticks to access pupil level data.

Free comments revealed a wide range of **inconsistent practices and levels of security.**

The rights of teachers (increasing workload, lack of training)

There is extensive research by academic Neil Selweyn, his colleagues and others, on what the hidden labour from staff means for workload – typically displaced not replaced– and raises the questions of what staff time and effort the state education system is providing "for free" to commercial product providers, often still in development when it comes to emerging tools such as Artificial Intelligence.

There has been some academic research on teacher workload, stress and burnout in the use of edTech in particular where there is no teacher training ahead of deployment and on use.

"Currently, there is interest in incorporating technology in the classroom due to the multiple benefits it can bring to students. However, the reality shows that its use may also be negative for teachers because it could imply changes in their teaching methods or pressure to acquire technological skills, leaving sequelae such as physical, social, and psychological problems."[18]

[17] 2018 survey of GDPR readiness in schools with a voluntary survey from 35 schools in England https://defenddigitalme.org/wp-content/uploads/2023/11/Survey-Monkey-staff-views-on-GDPR-readiness-in-schools.pdf

[18] US based research on edTech and teachers' health https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7827099/

The rights of parents

A 2018 poll of parents in England we commissioned found that only half of parents agree they have enough control of their child's digital footprint.

The State of Data survey was carried out for **the State of Data 2020 Report** by defend digital me, before the pandemic, online in 2018, between 17th and 20th February 2018. Survation polled 1,004 parents' opinions of children's data collection and uses of everyday technology in state education in England. Respondents were parents of state-educated children age 5-18 in England. They were asked detailed questions about their child's personal data in school, their understanding of which technologies were used, as well as questions about their attitudes towards the use of children's personal confidential data at national level by third parties

.As many as one in four (24%) parents said they do not know if their child has been signed up to any systems using personal data. When asked how often they were told if their child's personal data will be stored or transferred to third-party organisations through a school administration software or an online learning service, only 31% of parents said they were always informed of this. 23% said they were never informed of this while 10% of parents replied, "Don't know."

Over two thirds (69%) of parents said they had not been informed that the DfE may give out data from the National Pupil Database to third parties. Most strongly from all answers, parents appear to consider children's special educational needs data merits extra consideration, before a school passes that sensitive information on to the Department for Education (DfE) for secondary re-uses.

- 81% of parents agreed that parental consent should be required before a child's special educational needs data is shared.
- 60% parents agreed parental consent should be required before schools pass data to the DfE National Pupil Database.
- 65% agreed the Department for Education should have parental consent in order to pass children's personal data to commercial data analytics companies.
- Over three quarters (79%) if offered the opportunity to view their child's named record in the National Pupil Database would choose to see it. There is, in 2023, no communication of this process to parents and there is no process at all suitable for a competent child.

Legal guardians' / parental rights are grafted onto a child's right to education in many European and global texts including the UN Declaration of Human Rights, Article 26(3), "Parents have a prior right to choose the kind of education that shall be given to their children."

The rights of the child

The UNCRC demands policy makers aim to ensure every child is safe, has effective access to and receives education, services, and recreation opportunities - to develop **to their fullest potential.** Article 12 of the Convention on the Rights of the Child (the Convention) a right to be heard, is a unique provision in a human rights treaty; it addresses the legal and social status of children, who, on

the one hand lack the full autonomy of adults but, on the other, are subjects of rights. It is vital to balance the rights of safety, privacy, and participation.

The Council of Europe ("CoE") 2016-21 Strategy on the Rights of the Child,[19] devoted 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 *"paid to empowering children in vulnerable situations,* ***such as children with disabilities."***

It recognises in para 5.3. that "provision for children in the digital environment ICT and digital media have added a new dimension to children's right to education" exposing children to new risks in, "privacy and data protection issues"[20] and that "*parents* ***and teachers*** *struggle to keep up with technological developments."* UNICEF's recent working paper on children *Privacy, Protection of Personal Information and Reputation says*, "*it becomes evident that* ***children's privacy differs both in scope and application from adults' privacy.***"

In 2010, the CoE Committee of Ministers adopted Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, and made special reference to the harms of solely automated decision making and profiling, and recommended they were barred for children:

> *"The use of profiles, even legitimately, without precautions and specific safeguards, could severely damage human dignity, as well as other fundamental rights and freedoms, including economic and social rights.*

In the UK this has not happened, so if solely automated decision making and profiling should not routinely concern a child, to respect Recital 71 of GDPR, and the CoE Principle 3.5, "*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,"* there must be change in policy, in practice and strong codes for effective enforcement. Our children's future is being shaped by data, and through this legislation, by their safeguards or lack of them.

Companies rarely demonstrate adherence to the obligations to respect, protect and fulfil the rights of the child in the digital environment[21] and UNCRC General Comment No.16 (2013)[22] regarding the business sector's impact on children's rights.

The education of the child shall be directed, according to UNCRC Article 29[23], to the development of the child's personality, talents, mental and physical abilities to their fullest potential with respect for human rights, fundamental freedoms and principles. Children are also entitled to protection from economic exploitation under Article 32 of the UNCRC, to inclusive and equitable education opportunities for all, without discrimination. Article 24 of the UN Convention on the Rights of Persons with Disabilities, and the UN Convention on the Rights of the Child[24], ratified by over 197 State Parties worldwide, already offer a robust framework for protecting children's rights that should be applied by all parties in the adoption and use of digital learning tools.

General comment No. 5 on the implementation of the UNCRC emphasises that *"implementation of*

[19] Council of Europe Strategy for the Rights of the Child 2016-21 Para 37, p15/36 https://rm.coe.int/168066cff8
[20] Ibid. p10/26 (6) Para 21. And 28 EU Kids Online (2014), EU Kids Online: findings, methods, recommendations
[21] https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a
[22] https://sites.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf
[23] https://www.unicef.org.uk/rights-respecting-schools/the-rrsa/the-right-to-education/
[24] https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

the Convention is a cooperative exercise for the States of the world," and includes the obligation to ensure that non-State service providers also operate in accordance with its provisions.

UK children are unprotected from high-risk AI covered in the EU AI Act

A number of high-risk applications may involve remote biometric identification of pupils in (semi-) public places such as sports- or playgrounds and/or claim to perform emotion recognition cognitive profiling or social scoring – some or all of which may well be banned soon under the EU AI Act. In the UK there is no assessment of the risk of such tools, and children in UK schools will not have its protection.

Emerging generative AI and other automated decision making is being incorporated into psychometric assessments, but might pose a real risk where used to 'predict' students' future educational and career development.

Biometrics

In October 2021, there was outcry when schools in Scotland adopted facial recognition for routine canteen cashless payment systems. Read more in our briefing including the court and regulatory action in other countries including bans on biometrics in schools.[25] Read about the 2021 debates in the Scottish Parliament on October 28th and the House of Lords on November 4here; and the joint-action with Big Brother Watch and media coveragehere. In March 2023 the Welsh Senedd backed a call for legislation over the use of biometric data in schools led by Sarah Murphy, member for Bridgend. Now is the time to strengthen, not weaken biometrics oversight as planned in the upcoming Data Protection Bill through the scrapping of the Office of the Surveillance Camera commissioner, and biometrics in education needs dedicated specialist oversight.

> *"Despite repeated requests from the Biometrics and Surveillance Camera Commissioner to have legal oversight of the ethical use of that technology in schools, the Government have refused to agree. Why is this loophole still there, and when will it be closed?"*
>
> Lord Scriven, December 2022, The House of Lords

In the 2022 report, *The State of Biometrics 2022: A Review of Policy and Practice in UK Education*[26], Pippa King and Jen Persson mapped the prevalence of biometrics in educational settings based on original research from the four regions of the UK; England, Northern Ireland, Scotland, and Wales. Published on the ten-year anniversary of the Protection of Freedoms Act 2012, the report challenges the presumption that the law alone is effective in the protection of children's rights.

[25] Defend Digital Me Briefing on biometrics in UK schools April 2023 https://defenddigitalme.org/wp-content/uploads/2023/04/Biometrics-in-schools-briefing-2-April-2023.pdf
[26] The State of Biometrics 2022: A Review of Policy and Practice in UK Education https://defenddigitalme.org/research/state-biometrics-2022/

Some companies have claimed to be able to identify mood and emotions using "pose estimation" based on pupils' faces.[27] Others to be able to identify and profile "hidden social-emotional risks that might otherwise go undetected".[28]

The use of fingerprints for routine tasks in schools, such as buying lunch in the school canteen or borrowing a library book is commonplace. and facial recognition is growing, reportedly given free to schools who were existing customers of fingerprint technology as "an upgrade" but without any public information who makes, rather than distributes, the technology to schools or in which country it is manufactured. The report documents emerging technologies such as emotion and mood detection, as well as some of the myths and mistakes made by schools when adopting the products sold by a wide range of companies from around the world. With a foreword from the Biometrics and Surveillance Camera Commissioner Fraser Sampson, the report calls for a better approach and ban on biometrics in educational settings across the UK.

It concludes that In line with recent regulatory authority and court decisions on facial recognition in France and Sweden, and fingerprints in Poland, as well as various parts of the U.S. it is time to ban the broad use of biometrics in UK schools, from facial recognition and fingerprints in canteens to AI using bodily data to make inferences of emotional detection and attentiveness through articulated human pose estimation. Harm is already felt; from discrimination and infringement on human dignity in e-proctoring exams, to the imposition of biometrics policy or no food, on disadvantaged children in receipt of free school meals. Further risks to the rights and freedoms, and full and free development of the child, may not be fully realised yet.

We are not even close to understanding what VR and AR and haptics and neurotech means for schools, although brain scanning headbands and neuro-technology is widely marketed.

The normalisation and chilling effects of surveillance are already seen in trials. The potential effects and harms from undermining the importance of biometrics for later in life, in security, attitudes, and identity theft, are foreseeable.

DfE Lack of Assessment of biometric technology specs or standards

In answer to a number of parliamentary questions asked in 2021, it is clear that the Westminster Department for Education, despite offering guidance to schools, holds no information on standards or specifications of any hardware or software of biometric technology used in UK schools, nor its suppliers, or any understanding of the level of intrusion in common tools used e.g. iris / palm scanners. These can be seen in one place online via our website.[29]

[27] ViewSonic's myViewBoard Sens Brings UK's First AI-powered Classroom to Smestow Academy https://web.archive.org/web/20230810120916/https://www.viewsonic.com/uk/presscenter/content/viewsonics-myviewboard-sens-brings-uks-first-ai-powered-classroom-to-smestow-academy_4823

[28] Defend Digital Me (2020) See case study 3.10.4 Socio-emotional mental health tracking | Case study STEER AS Tracking https://defenddigitalme.org/research/the-state-of-data-2020/report/

[29] State of Biometrics 2022 https://defenddigitalme.org/research/state-biometrics-2022/#chapter-10 Appendix A: FOI requests analysis from schools 2021-22

Date asked	Authority	Response	Reference
28/07/2021	The Department of Education (Westminster)	The DfE does not hold any information on **standards or specifications of any hardware or software of biometric technology used in UK schools.**	Link
28/07/2021	The Department of Education (Westminster)	The DfE **does not hold any information about suppliers** that provide biometric technology to schools.	Link
28/07/2021	The Department of Education (Westminster)	The DfE **does not hold any information about the types of biometrics that are used in schools.** i.e. fingerprints, facial recognition, palm, vein or iris scanning.	Link
17/09/2021	The Department of Education (Westminster)	Nor do we provide advice to providers of such [facial recognition] technology. The department's publication [1]Protection of children's biometric information in schools explains the legal duties schools and colleges have if they wish to use biometric information about pupils. (But fails to mention this is long out of date). 2) Please provide your advice to companies which are providers to schools and schools/educational establishments wishing to use facial recognition technology. (This would include advice ref GDPR and Data Protection Act 2018). 3) Please advise if you have been approached by any companies wishing to supply facial recognition to schools and provide all communications you have had with them, this includes all communications, i.e. minutes of meetings, letters, emails, video calls, etc.	Link 1 Link 2 The above 'Protection of Children's Biometric Information in Schools' is out of date. Last update was March 2018 and cites the DPA 1998 4 times, no update on DPA 2018 and GDPR. Needs updating.
02/09/2021	Information Commissioner's Office (ICO)	• Advice to companies • Working with companies • Facial recognition hardware and software standards to be used in educational establishments?	Link
08/09/2021	Education Scotland	Government does not have the information [on facial recognition in schools] you have requested.	Link

DfE Due diligence of its accredited edTech tools for Early Years (children age 2-5)

On February 21, 2020 the Department for Education announced the promotion of six apps for Early Years children at home and in Early Years educational settings.

On the **Hungry Minds website** the DfE[30] instructs adults to download the products[31] as part of the government's drive to help parents make informed decisions about the use of technology in creating positive learning environments at home.

The expert panel that accredited the apps, appointed by the Department for Education, included children's digital media consultants, early learning charities and researchers at universities. However it was not in their remit to consider any child rights, data protection or privacy impact assessment, or to carry out due diligence of the companies and their data processing or financial structures for example. This approach may not be sufficient to support families to make informed choices when the accreditation through the Department for Education may come with an assumed level of safety and quality standards. Notable gaps in transparency include privacy policies for one AI product in which there is no information at all about what data is used in the AI algorithms, nor how the child's data may be being used to develop and train the product, or what its training data set was and how data is used ongoing. Another was based in Hong Kong without any impact assessment of the implications

[30] https://defenddigitalme.org/research/the-state-of-data-2020/report/#ftnt306
[31] https://defenddigitalme.org/research/the-state-of-data-2020/report/#ftnt307

for payment or data transfers outside the UK. One was an unfinished product still at research trial stage, another run by a new university graduate without any obvious credentials in education or evidence of their trustworthiness to be an accredited product given state-accredited access to family life.

DfE supported research trials may not respect standard public interest research ethics

Children's data was collected at scale in a voice-data based trial in collaboration between Nesta, the DfE, SSAT, the University of Melbourne Australia, and AI-media (part owned/ funded at time by the UK Behavioural Insights Unit). There are open questions on the lawfulness of the biometric data processing, on the research ethics of parents required to take part as part of everyday education, and of their data extracted from the national pupil database at the DfE without consent to be used in a project for a commercial product development, not public interest research.

Since 2013 the Visible Classroom project has used audio recordings from UK schools' lesson, "As part of our [Nesta] technology in education programme trialling different types of digital technology in schools and exploring its potential for learning."

A key purpose for this research was commercially driven. As Nesta described in 2015:

> **"Based on this work with teachers and students, Ai-Media UK have been able to develop 'The Visible Classroom' further into a refined product for supporting teacher professional development. What was a new technology not tried in schools in this format before, has become a product that can be rolled out to schools**."

The project also extracted data from the Department for Education National Pupil Database in order to examine the impact of the programme on reading and mathematics attainment, measured using KS2 SAT performance in Reading and Maths. The initial intervention was designed as a two-armed randomised controlled trial, involving 140 primary schools but some pupils "were randomised into the trial prior to confirmation that opt-out forms had been distributed", and where it was too late to offer families opt out, since, "the Year 6 cohort had by this point already moved on to secondary."[32]

The control of rights to the audio recordings were completely owned contractually by the company in perpetuity.

> "..by uploading audio recordings to the App, you hereby grant us and our affiliated companies a non-exclusive, worldwide, royalty free, fully paid up, transferable, sublicensable,

[32] Statistical Analysis Plan 05.06.2018. See section Missing Data p8 https://educationendowmentfoundation.org.uk/public/files/Projects/Visible_Classroom_SAP.pdf (the original report is no longer accessible on the EFF website but was archived by Defend Digital Me) https://web.archive.org/web/20211012105019/https://educationendowmentfoundation.org.uk/public/files/Projects/Visible_Classroom_SAP.pdf

perpetual, irrevocable license to copy, display, upload, perform, distribute, store, modify and otherwise use your audio recordings and the transcripts in connection with the provision of the Services and otherwise contemplated under these Terms of Service, in any form, medium or technology now known or later developed."

Threats to learners and teachers from commercial product development labelled as "research"

There is a growing divide between public interest research standards and "commercial" research. This has been encouraged through the 'research for all' approach of the Research Schools and other intermediaries undertaking activities classed as research but that do not follow the same research protocols or standards necessarily that would be recognised by academic bodies. The Think Tank **Nesta has told schools that there is no need to ask for consent[33] to sign up thousands of children into edTech trials across a range of products, as part of their regular education.** This is not only likely to breach data protection and privacy obligations because of the commercial products accessing and using personal data, but is contrary to British Educational Research Association (BERA) recommended practices on informed consent, and good research ethics.[34] But it has become routine for children and parental objections to be ignored when children are required to participate in a randomised control trial in schools. This is an example of why, although data protection law may offer a mechanism to protect privacy from outsiders to a school, it is not enough to prevent interventions in children's lives which the providers refuse to make transparent, and therefore Data Protection law alone is inadequate to protect children's rights and freedoms in a coercive setting.

Another such case study is given in the State of Data 2020 report, of a trial carried out involving over thousands of pupils across England, across 60 schools involved in the Social Cohesion study led by **the Behavioural Insights Unit** ("BIT") and commissioned by the Ministry of Housing, Communities, and Local Government (MHCLG). Full details can be read online.[35]

Without full transparency of what was involved in the intervention, Defend Digital Me (Jen Persson herself also in a private parental capacity) requested an opt out from the trial which was refused, and also collection of her children's personal data in the trial, including religion (sensitive personal data). She asked the school for a copy of the study's Data Protection Impact Assessment, Legitimate Interests Balancing Test, and Research Ethics paperwork. The school did not have copies of these itself and could not provide them, even though they had agreed to the trial. The Behavioural Insights Unit refused to provide copies, although acknowledged that research ethics had been provided by an institute in Portugal. The BIT has no relationship with families at all. Most families are unlikely to know what the BIT is as an organisation or have heard of the University of Lisbon's School of

[33] Nesta edTech innovation testbed FAQs for schools involved, on their website: "there is no need for individual consent". https://www.nesta.org.uk/project/edtech-innovation-testbed/frequently-asked-questions/
[34] Ethical Guidelines for Educational Research, fourth edition (2018) https://www.bera.ac.uk/publication/ethical-guidelines-for-educational-research-2018-online#privacy
[35] Search for 3.11.5 Case study | Interventions without consent | The Behavioural Insights Team in the State of Data 2020 Report https://defenddigitalme.org/research/the-state-of-data-2020/report/

Economics and Management, “our research partner in this project”. How children’s behaviour was changed and the contents of the trial, opaque at best.

Generative AI

In the face of foundational models and Generative AI, the education sector is challenged by how to respond to the potential for plagiarism, threats to academic integrity and from inaccurate, inappropriate, biassed, unreliable text generators that may offer out of date information, and be used out of context without permission.[36] The DfE guidance on generative tools fails to address the question of whether such tools can be used lawfully by pupils or staff in a non-consensual environment where consent is the only basis for data processing offered by the companies.

There is widespread ignorance of products' own policies on children’s use, for example to use ChatGPT (https://chat.openai.com) you must be at least 13 years old and if you are under 18 you must have your parent or legal guardian’s permission to use the Service. Valid consent for a learner, especially a child, to use edTech is almost impossible to achieve for routine classroom or homework activity. (see intro. Open questions point 2)

Based on the 2019 G20 AI Principles, the OECD developed five principles and five recommendations for policy makers covering transparency, explainability, accountability, human involvement, and protecting data when it comes to AI. The OECD has identified that the biggest challenge is creating and maintaining trust. This is true from a position of everyday teaching as much as for concerns of academic integrity and qualifications. However there is no independent evidence to date on whether in fact generative AI generated material interferes with assessment and exams.e-proctoring on the other hand is well documented and there is significant push back including legal action led by students and staff in many parts of the world. The Council of Europe (relevant to the UK as a Member State) also has a programme of work underway on AI and education.[37]

But the fundamental failings of companies to meet the 7 data protection principles, starting with lawfulness and telling people what you do with their data seem to fall flat at the first test. The ICO has issued guidance[38] *Generative AI: eight questions that developers and users need to ask* and the Global Privacy and Data Protection Authorities issued a joint resolution in October 2023.[39]

> “Generative AI systems must have a legal basis and be lawful in accordance with applicable legislation even when personal data is publicly accessible.”

[36] DfE guidance on generative tools fails to answer whether they can be used lawfully by pupils (2023) https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education

[37] Jen Persson (DDM director) is a member of the CoE working group on AI and education and co-author of the report AI and education - A critical view through the lens of human rights, democracy and the rule of law (2022) https://rm.coe.int/artificial-intelligence-and-education-a-critical-view-through-the-lens/1680a886bd

[38]https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/generative-ai-eight-questions-that-developers-and-users-need-to-ask/

[39]https://globalprivacyassembly.org/wp-content/uploads/2023/10/5.-Resolution-on-Generative-AI-Systems-101023.pdf

Large Educational Platforms

Case study: Google Classroom, formerly, G-Suite accounts are ascribed to a child in school, both in primary and secondary schools across the UK. The child and parents have no meaningful way to object, since the tool is the way the school has chosen to share documents with the child, assign homework, and staff and children communicate via school assigned gmail accounts.

In Wales, at the start of the Covid-19 pandemic, the Welsh Government via Hwb (March 23, 2020[40]) said 'Previously, these services have only been made available where learners or their parents/carers had given consent, from Monday 23 March 2020, schools will no longer rely on consent,' but also said that the decision would be reviewed once the crisis was over. We do not believe that review has been carried out and parents who complained at the time of the requirement imposed, have not had any opportunity since to object.

The system is in effect split into two sets of bundled services: Core services, and Additional services. Google says that user personal information collected in the **Core Services** is used only to provide the **Core Services** like Gmail, Docs, Sheets, and Slides. However information from all Additional **Services** can be used to provide, maintain, protect and improve them, and for product development. This also includes the re-use of children's personal data, collected without valid consent in the course of required classroom activities, for the company's development of its LLM training datasets for AI.

Large EdTech companies appear to give up their reach into children's lives only unwillingly. Google has made concessions to the education sector in the Netherlands and to respect children's rights but not in the UK:

> *"In May 2021, the Dutch Data Protection Authority warned that schools could not use Google Workspace for Education in the new 2021 academic year, as a report by consultancy Privacy Company in 2020 indicated high privacy risks emerging in particular from the telemetry and diagnostic data that Google collected for its own purposes and analysed beyond the context of the contracting school. Against this backdrop of a potential prohibition, the Dutch cooperative of school boards for ICT purposes, SIVON (and the equivalent organisation for higher education, SURF) engaged in negotiations with Google. It obtained an agreement that Google would move from being a (joint) data controller, and that it would process personal data of students and staff for 33 of its own purposes, to a data processor, where it would only be able to process data for three narrow, pre-agreed-upon purposes on the explicit instruction of the school (Nas & Terra, 2021). Interestingly,* ***this agreement appears to be only operational in the Netherlands through a contractual amendment, indicating the***

[40] Welsh Government Hwb (March 23, 2020) statement on Google Classroom https://web.archive.org/web/20200331085316/https://hwb.gov.wales/news/article/76979aea-3819-42e9-9c10-121e907ef922

reluctance of Google to distribute the negotiated benefits elsewhere."

(Veale, 2023)[41]

What products may do has no limitations or oversight

Without any consistent or comprehensive evaluation framework for robustly auditing products, settings cannot assess whether or not EdTech products are effective, or that they are lawful, safe, and rights' respecting over a product or data lifecycle. There is no oversight of widespread monitoring, profiling, data mining, marketing[42], or manipulation of children or school agreements for commercial exploitation. The Department for Education should consider the independent assurance organisation this requires and put the necessary infrastructure in place.

Educational stability and the impact school infrastructure and children

Educational institutions may be customers, when children are the users of their products but never see the terms and conditions for using a product. Terms and conditions or its costs can often change without redress at short notice. There is no Service Level Agreement between companies and children, and no assessment available of the impact on a child's experience of learning, or their outcomes, If a product is bought out or discontinued. Can products be allowed to simply shut down with consequences for the stability and sustainability of state education systems if school infrastructure or its delivery depend on these external actors? These are not only tools for learning but nudging behaviour and mental health and children may have developed dependencies on such tools in a range of ways.

Robots

As robots become more everyday in the classroom, for example to support childrens 'engagement and agency in storytelling with a 'social robot'[43] there are questions as yet under-researched on the effects on **child development**, influencing children's voice patterns, social interactions, and questions over the embedding of gender stereotypes through machines' physical form, their given voice and behavioural responses.[44] The danger is that designing hardware toward current stereotypes can reinforce those stereotypes. This is all on top of the "surveillance by sensors" constant image recording,[45] and data questions.

[41] Veale, M. (2023) Schools must resist big EdTech – but it won't be easy https://educationdatafutures.digitalfuturescommission.org.uk/essays/competing-interests-in-education-data/schools-must-resist-big-edtech

[42] Human Rights Watch, "How Dare They Peep into My Private Life?" – Children's Rights Violations by Governments that Endorsed Online Learning in the Covid-19 Pandemic, 25 May 2022, available at: https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

[43]https://research.vu.nl/ws/portalfiles/portal/121657682/Design_patterns_for_an_interactive_storytelling_robot_to_support_childrens_engagement_and_agency.pdf

[44] https://genderedinnovations.stanford.edu/case-studies/genderingsocialrobots.html

[45]https://www.dailymail.co.uk/news/article-11562599/Robot-vacuum-cleaner-took-photos-woman-toilet-images-ended-Facebook.html

Adtech

Processing children's data obtained via EdTech may be monetised in a number of ways, and not by "selling the data" which is often a red herring to indicate safe processing by third parties. One method is powered by the advertising technology (AdTech) industry. As Human Rights Watch reported on their research about what common EdTech tools do, in 2022[46]:

> *"Most online learning platforms sent or granted access to children's data to third-party companies, usually advertising technology (AdTech) companies. In doing so, they appear to have permitted the sophisticated algorithms of AdTech companies the opportunity to stitch together and analyse these data to guess at a child's personal characteristics and interests, and to predict what a child might do next and how they might be influenced. Access to these insights could then be sold to anyone—advertisers, data brokers, and others—who sought to target a defined group of people with similar characteristics online."*

Children are surveilled at dizzying scale in their online classrooms. Human Rights Watch observed 145 EdTech products directly sending or granting access to children's personal data to 196 third-party companies, overwhelmingly AdTech.

The commercialisation of children through adTech might **not only be measured in terms of commercial benefit to advertisers** but also in the cumulative **learning loss** to the child.

> *"My son aged 9, is using Read Theory, which has been recommended by the school, but every few minutes adverts for Disney keep popping up and he cannot stop himself from watching them. In fact he seems to spend more time watching the adverts than he does on the work." (Defend Digital Me, State of Data 2020 Report)[47].*

Marketing

Case study: Class DoJo, a classroom app, links from its own webpage to an article from September 2016, How Class Dojo plans to Make Money having been freeware distributed to children through schools:[48]

> *"Having connected parents and teachers, five-year-old ClassDojo is now beginning to turn its attention to the next part of its journey: monetizing the service. The company said it has no plans to sell advertising. Instead, ClassDojo is looking at selling educational content. With access to so many teachers and students, the startup is leveraging its distribution capabilities to spread educational videos to an audience of teachers and students on a level that's never been seen before."*

[46] Human Rights Watch, "How Dare They Peep into My Private Life?" – Children's Rights Violations by Governments that Endorsed Online Learning in the Covid-19 Pandemic, 25 May 2022, available at: https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

[47] Defend Digital Me (2020) State of Data report Case Study 3.8.4.13 18:00 Case study: Advertising | Read Theory https://defenddigitalme.org/research/the-state-of-data-2020/report/

[48] ClassDojo Wants to Do for Education What Netflix Did for Enter (Inc.) https://www.inc.com/salvador-rodriguez/classdojo-monetization-slack-classrooms.html

> *"It's a huge distribution platform to reach parents," Don said. "We want to, In the long term, enable parents to be consumers for their child's education."*

Essentially it is a “freemium” model, in which users are given the basic tools to use the service, but for those willing to pay, more content is added to enhance the experience.In 2020, there were company plans for this model to be based off and tailored to, a user location.

Where do products come from or send pupil data to?

The old adage of ‘follow the money’ to understand a business, is as true in EdTech as other areas. While the business insights business Holon IQ is showing venture capital funding down below pre-pandemic levels.[49] Significant parts of the UK EdTech infrastructure in schools is controlled by a small but significant number of global players with transnational investments (ie Google, Microsoft and Apple), but the SME market is significant, with EdTech venture capital funding coming mainly from the U.S. and China, and a growing export influence from India.

The collective power from data concentration in a few product owners is reinforced by significant mergers and acquisitions in the education sector, such as the Anthology and Blackboard (common in UK Higher Education) $3 billion merger in 2021. There is a serious risk of dominating platforms cornering the market and the ability to develop AI-based EdTech giving them undue authority in the sector, with significant implications for the sustainable delivery of the infrastructure of state education and the development of an open, innovative economy.

Education infrastructure might be said to be overly reliant on edTech companies outside England, with opaque future costs, controls, or guarantees of security and stability for the delivery of education. Digital environments can change rapidly. Data is passed around at speed and scale. Companies may be bought out by investors, and ownership transferred in foreign takeovers multiple times in the course of a child’s education. Companies' oversight boards may change overnight. The school may be asked to accept new terms and conditions without any choice or face losing core systems. One popular reading tracking app[50] serving 20 million students in 45,000 schools in more than 90 countries worldwide, is owned by a Cayman Island based company with thousands of affiliate companies. “We will not pass your data to third parties”or ‘data is not monetized’ in Terms and Conditions becomes near meaningless in such cases.

The UK Data Protection and Digital Information Bill

The upcoming Data Protection and Digital Information Bill could be an opportunity to better safeguard children in the face of foundational models whose developers have built their tools by indiscriminately scraping facial images and poses from photos at scale, and using them to “train” tools that are then the infrastructure on which AI generated images can be shaped to generate lifelike or even look-a-like pornography or CSAM.[51]

---

[49] https://www.holoniq.com/notes/904m-of-edtech-vc-in-q3-2023-strong-series-b-c-market-everything-else-down-50

[50] See case study 3.8.4.11 16:00 Case study | The reading monitor | Accelerated Reader in The State Of Data 2020 report https://defenddigitalme.org/research/the-state-of-data-2020/report/

[51] 404Media (2023) Andreessen Horowitz Invests in Civitai, Which Profits From Non-consensual AI Porn https://www.404media.co/andreessen-horowitz-invests-in-civitai-key-platform-for-deepfake-porn/

Yet the UK government in its March 2023 white paper, 'A pro-innovation approach to AI regulation' (updated 4 July 2023), said it does not initially intend to introduce new legislation regulating artificial intelligence (AI) because of the potential impact on businesses. We need impact on these businesses. Their CEOs and funders[52] may prefer an unregulated world, in which they do not believe, "that freedom and democracy are compatible"[53] in which they try to fend off the inevitability of death, and should the world become uninhabitable, retreats in New Zealand, seasteading and even space offer the hyper-rich a way to escape, backed by "the creation of a new world currency, free from all government control and dilution"[54]. But others' attempts at such "worldcoin" products, have been found to breach data protection laws abroad[55], and caused concern in the UK[56] as well. Our public sector infrastructure, the delivery of health and education systems, must be protected from such worldviews if we are to uphold the public above private interests.

The upcoming Data Protection and Digital Information Bill fundamentally refocuses the essential nature of the UK data protection regime. It moves away from today's rights-based regulation, which prioritises seven key data protection principles framed by accountability as an overarching premise, towards a business-centric one, in which accountability is downgraded as part of its deregulation aims. This leaves people, including children, less protected.

"Successful sustainable innovation is dependent on building and maintaining public trust."

The Centre for Data Ethics and Innovation Review into bias in algorithmic decision-making 2020).[57]

Every time the Bill is described as "reducing the compliance burden on businesses" substitute "stripping today's data protection safeguards from children." Now is the wrong time for downgrading data rules if the UK is serious about becoming a "tech super power".[58] Regulation is going in the wrong direction by reducing safeguards against data misuse while the sensitivity of our personal data collected and the automated methods for its use and abuse at speed and scale go up.

> *"Genesis Market had **80 million sets of credentials and digital fingerprints up for sale, with the NCA calling it "an enormous enabler of fraud".** Genesis Market sold login details, IP addresses and other data that made up victims' "digital fingerprints"."*
>
> (BBC News, April 5, 2023)

The paradox could not be more stark if one remembers the DCMS motto of the Online Safety Bill on

[52] https://web.archive.org/web/20231120062118/https://civitai.com/articles/2976/weve-raised-dollar51m-in-seed-funding-led-by-andressen-horowitz
[53] Peter Thiel Cato Unbound(2009) https://www.cato-unbound.org/2009/04/13/peter-thiel/education-libertarian/
[54] https://www.cato-unbound.org/2009/04/13/peter-thiel/education-libertarian/
[55] Kenya (2023) Kenya becomes the first country to suspend Sam Altman's Worldcoin A.I.-crypto scheme https://fortune.com/2023/08/02/kenya-first-country-to-suspend-worldcoin-altman-privacy-orb-iris-crypto-ai/
[56] Reuters (2023) UK data watchdog to make enquiries about Worldcoin crypto project https://www.reuters.com/technology/uk-data-watchdog-make-enquiries-worldcoin-crypto-project-2023-07-25/
[57] The 2020 CDEI Review into bias in algorithmic decision-making (p6) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf
[58] DSIT (March 2023) International Technology Strategy to guide the UK to becoming a tech superpower by 2030. https://www.gov.uk/government/news/plans-to-make-uk-an-international-technology-superpower-launched

the one hand, *making the UK the world's 'safest' place to go online*, rendered pointless if on the other hand, this Bill increases their digital risk with lifetime impact in an increasingly digitised world.

> *"inappropriate data processing practices by e-learning platforms, opaque automated decision-making and misuse of learning analytics, risk undermining data protection and privacy rights. In the case of children and youth, this can have* ***significant and long-term social, economic and professional consequences****, and fail to account for their evolving capacities."*
>
> (Resolution from the 2018 International Conference of Data Protection and Privacy Commissioners.)[59]

[59] https://edps.europa.eu/sites/default/files/publication/icdppc-40th_dewg-resolution_adopted_en_0.pdf

Proposal for a Code on processing personal data in education

A Code of Practice has been proposed a number of times since the introduction of the GDPR in 2018.

This would require theInformation Commissioner to produce a code of practice, pursuant to GDPR Article 40(g), relating to the rights 40 (a)-(k) as specific to children (up to age 18 for purposes of GDPR except where stated in the Bill) and pupil (as defined by the Education Act 1996, who may be up to age 19 and 25 where recognised as having additional SEND needs). The obligations of schools and data controllers appropriate to children's age, type of education and capacity, need clarity and consistency.

In 2017, Lord Clement-Jones said at Committee stage on the UK Data Protection BIll (2018), [Col 1865], on Article 22 and safeguards, "*the provisions related to automated decision-taking should not be allowable in connection with children. That requires clarification*." Obligations specific to children's data, especially regards "solely automated decision making and profiling," and exceptions, need to be consistent, with clear safeguards-by-design where they restrict fundamental freedoms.

A code is needed a) because the safeguards are missing that GDPR or Convention 108, as both apply to the UK, that are required in several places. A code should breathe life into the explicit recommendation of the Working Party 29 to create guidance on automated decision-making with significant effects and profiling in the GDPR Recital 71, such a measure 'should not concern a child' and principle ofRecital 38, that children "merit specific protection." The WP 29 wrote ***"Article 40(2)(g) explicitly refers to the preparation of codes of conduct incorporating safeguards for children;"***

For common case studies of profiling in education in England see our submission to WP29.[60]

Much debate has been around child protection, not their data protection. While integral to one another in online safety, these protections are also distinct from one another. Although the broader debate of ethical principle is outside this debate, some of the interpretative value judgements of Recitals specific to children under GDPR must be embodied in a manner understandable for everyone in a data ecosystem, if we are to see anything happen. If not, uncertainty and unwillingness to cooperate in a responsible and interoperable manner, will make the whole process of child data flows unworkable; and impossible for a child to manage their digital footprint.

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

2. Lawful basis for edTech, in particular emerging technologies and AI: Schools give children's personal data to many commercial companies during a child's education. It cannot be based on valid consent, Article 6(1)(a) or 8(1), when it comes to education because of the nature of the non-consensual environment with a significant power imbalance that affects the 'freely

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

give' nature of consent, and that cannot be refused without detriment for routine educational activities; but despite this, consent is often said to be assumed by schools on behalf of companies, "*for the performance of a task carried out in the public interest*." A code should clarify any boundaries of this legal basis where it is an obligation on parents to provide the data, and what this means for the child on reaching maturity and after education.

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

4. Children and those with parental responsibility must be supported to understand the effect of the responsibilities of controllers and processors, for the execution / limitation of their own rights.

5. The Article 29 WP further recommends, "*Because children represent a more vulnerable group of society, organisations should, in general, refrain from profiling them for marketing purposes.*" What will this mean for software platforms that profile users meta-data to share with third parties, or commercial apps signed-up-for in schools that offer advertisements in-use, or bait and switch premium model?[61]

6. Setting out child appropriate safeguards is necessary under GDPR Articles 13(2)(f), and 21-23 for exemptions. Current UK data protection law fails to set out any required safeguards designed for children.

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

8. Joint-controllers treat the same data differently. Schools need guidance on compliance where i) processing data under instructions from the controller(s) may differ from their own need and ii) there is a potential conflict in the best interests and restriction of the fundamental freedoms of the child, as regards mass export and re-use of school census data.

9. Further important rights the amendment addresses include with reference to GDPR Article 40:
(h) the measures and procedures referred to in Articles 24(3) (responsibility of the controller) and Article 25 (especially *"by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons")* as per Clause 55 (5) of the Bill, and retention periods, and measures to ensure security of processing (Article 32);
(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
(j) the transfer of personal data to third countries or international organisations;

10. Until 5 years ago, Subject Access was restricted by the Department for Education today

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

through the Research, History and Statistics exemption (section 33(4) of the DPA), to personal data in the national pupil database (ref. PQ108573) GDPR Recital 63 states that a data subject should have the right of access to personal data, collected concerning him or her, at regular intervals, in order to be aware of and *verify the lawfulness of processing. (Case C-141/12).* Will the Department ensure a process that is suitable for children and families to exercise this right?

Limitations and definition of a Code of Practice

- Education is devolved. Compulsory education ages are different and the issue of being in compulsory education and 18 does not arise elsewhere.
- A code does not prevent guidance being provided for use elsewhere. It would however clearly be welcome if consistently child rights as regards data were shaped to apply across the UK.
- In the Education Act 1996, "pupil" means a person for whom education is being provided at a school, other than—
    (a) a person who has attained the age of 19 for whom further education is being provided, or
    (b) a person for whom part-time education suitable to the requirements of persons of any age over compulsory school age is being provided.

With the meaning "pupil" ICO can recommend and consider capacity appropriate standards not only on age, but in the best interests of every pupil, within the meaning of the 1996 Education Act[62]. Beyond this, there are also pupils in education, for whom parental responsibilities and oversight of their children's rights and best interests can continue up to age 25 withSEND and an EHC plan in education. While SEND legislation takes account of this, this Bill without mention of capacity rather than age, does not.

Data protection cannot offer a tool that covers what is missing in its entirety to consider the issues of procurement and health and safety quality and teaching pedagogy, the influence of products on behaviour and values; and the legislative underpinnings and obligations of public law, administrative and equality legislation.

[62] The Education Act (1996) meaning of "pupil" http://www.legislation.gov.uk/ukpga/1996/56/section/3