Written evidence from Defend Digital Me (TEB28)

Public Administration and Constitutional Affairs Committee
Transforming the UK's Evidence Base inquiry

Introduction

In 2017, the then Children's Commissioner wrote in her report, *Growing Up Digital*,

> *"we are failing in our fundamental responsibility as adults to give children the tools to be agents of their own lives."*[1]

Nowhere is it more reprehensible than as a result of their state education and care. Children have no control over data processing decisions about them, taken by public bodies. There is no national appreciation of the sensitivity of longitudinal pupil records, how the education system structures fit together, where roles and responsibility and therefore accountability and oversight rest, or how they interact. These gaps contribute to poor data management practices and invisible ignorance. Schools don't know what they don't know and parents do not know where to look for information.

We call for urgent attention and action in key areas of data across the educational sector:

1. **Access and inclusion**: Accessibility design standards, Internet access and funding
2. **Data cycle control, accountability and security**: mechanisms are needed by industry and schools for lifetime data management including when children leave schools and leave education, and that restore lifetime controllership to educational settings
3. **Data rights' management:** A consistent rights-based framework and mechanisms to realise children's rights is needed between the child / family and players in each data process; schools, LAs, the DfE, companies, and other third-parties for consistent, confident data handling; right to information, accuracy, controls and objections.
4. **Human roles and responsibilities:** The roles of school staff, parents/ families and children need boundaries redrawn to clarify responsibilities, reach of cloud services into family life, representation; including teacher training (initial and continuous professional development).
5. **Industry expectations**: normalised poor practice should be reset, ending exploitative practice or encroachment on classroom time; for safe, ethical EdTech product development and SME growth.
6. **Lifetime effects of data on the developing child**: The permanency of the single pupil record must be reviewed given data law obligations on pseudonymisation over time.

[1] *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

7. **Machine fairness**: Automated decisions, profiling, AI and algorithmic discrimination.
8. **National data strategy**: The role of education data in the national data strategy and the implications of changes needed in the accountability and assessment systems.
9. **Procurement routes and due diligence**: Reduce the investigative burden for schools in new technology introductions and increase the independent, qualified expert support systems that schools can call on, benefiting from scaled cost saving, and free from conflict of interest.
10. **Risk management of education delivery:** Education infrastructure must be placed on the national risk register, reducing reliance on Silicon Valley tech giants and other internationally sourced tools and increasing transparency over future costs, practice, and ensuring long-term stability for the public sector.

1. The state of data processing in the public sector landscape: Education

1.1 Since 2015, we have researched personal data processing flowing into, across and out of the state education system in England. We published a comprehensive overview in the State of Data 2020: Mapping a child's digital footprint in the state education landscape in England[2] .

1.2 We conclude among the findings, that current national-level collection through the Department for Education ("DfE"), processing and re-uses, data distribution, linking and giving away of school children's personal data to third parties goes far beyond parents' expectations and what is fair. It is neither accessible nor foreseeable and often opaque when not explicitly covert.

1.3 The ICO noted[3] in its work for the 2020 audit of the DfE, that many parents and pupils are either entirely unaware of the school census and the inclusion of that information in the National Pupil Database" or are not aware of the nuances within the data collection, such as which data is compulsory and which is optional," and as such, "Our view is that the DfE is failing to comply fully with the GDPR in respect of these articles and the requirement for accountability in the processing of personal data."[4]

1.4 The DfE has been giving away 23 million people's identifying personal confidential data since 2012. They have neither informed people those parents of children in educational settings today, nor those who left school before the law was changed in 2012 to reuse the data the Department had already collected. Millions of people's pupil records are being

[2] The State of Data 2020:Mapping a child's digital footprint in the state education landscape in England. https://defenddigitalme.org/research/the-state-of-data-2020/report/
[3] Schools Week (2019) https://schoolsweek.co.uk/dfe-facing-action-over-wide-ranging-and-serious-data-protection-breaches/
[4] ICO Audit of the DfE https://defenddigitalme.org/2023/10/07/the-ico-audit-of-the-department-for-education-three-years-on/

given away to companies and other third parties, for use in ways we do not expect. In 2015, more secret data sharing began, with the Home Office. A pilot in data matching was run in 2018 with the DWP and pupil data has been given on occasion in a bulk data sharing to police.

1.5 The data when released to third-parties, are not anonymous, but are detailed, sensitive[5] and identifying.[6] Each release can include several million individual records. As Schools Minister Nick Gibb confirmed in January 2018 that,

> "*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.*"

1.6 There is no transparency of the volume of how many children's data have been given away in each approved release, because, "*the Department does not maintain records of the number of children included in historic data extracts.*" (PQ109065)

1.7 The Department is aware that they share and distribute too much data with third party users, calling it an 'excessive' amount of data in the underlying datasets'.[7] *"Users are required to download the entire dataset, then remove and manipulate extraneous data reducing it to a specific subset. Many expressed a desire to be able to customise the data they downloaded."*[8]

1.8 Access to children's education data carries not only individual but collective risk to the State. Knowledge of how pupils learn obtained through edTech data analytics is business intelligence, the gateway to knowledge and control of the entire state education system. That knowledge is produced today for free by the teachers and children who spend time administering and working in these digital systems and is passed on to the owners of companies around the world.

1.9 In addition to the public administrative data landscape, an increasing number of private commercial actors are supplementing state data infrastructure in critical and changing ways. For a variety of motivations, the rapid expansion of the number of commercial actors in the $8bn global edTech market[9] is vast and propagated not only by angel investors and tech accelerators in the US and the UK English language markets[10], but across the world. Over

---

[5] Sensitive data include SEND data, ethnicity and reasons for exclusions http://defenddigitalme.com/wp-content/uploads/2018/01/reasons_exclusion.jpg

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

[7]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721729/HiveIT_-_DfE_dissemination_discovery.pdf *DfE data dissemination discovery report,* 2018 (p29)

[8] DfE data dissemination discovery report, July 2018 (Page 29) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721729/HiveIT_-_DfE_dissemination_discovery.pdf

[9] UNICEF, Discussion Paper Series: Children's Rights and Business in a Digital World (p5) Privacy, Protection of Personal Information, and Reputational Rights https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf

[10] EDUCATE https://educate.london/

40% of edTech venture capital funding came from China in the last year, and the same share from the U.S. We need to get far more transparency from companies over their business models and future plans for freeware and the stability, sustainability, and national security of the state education system.

2. Protecting privacy and acting ethically: about national pupil data

2.1 There is a democratic deficit in how data is controlled in the education sector, which is a non-consensual environment and a special environment when it comes to data protection practice, because consent is almost never a lawful basis for routine data processing tasks and the data subjects are routinely children, still in development into adulthood, and without agency.

2.2 Imagine England's school system as a giant organisational chart. What do you see? Which institutions does a child physically pass through from age 2 to 25? How do the organisations relate to one another and who reports to whom? Where is regulation and oversight and where do I go for redress if things go wrong? It is nearly impossible for parents to navigate this real-world complexity amongst the last decade of restructuring of the state school system. Now add to that the world we cannot see. It is hard to grasp how many third-parties a child's digital footprint passes through in just one day. Now imagine that 24/7, 365 days a year, every year of a child's schooling and long after they leave school. (see 11.)

2.3 **Privacy isn't only a human right but a tool to protect individuals' lives, their human dignity and their future selves**. We must build a system fit to manage national administrative datasets safely to move forwards to meet the social, cultural and economic challenges young people face in a world scarred by COVID-19 and as we exit the European Union. We must not model our future aspirations for the economy and education on flawed, historic data and yet increasingly that is what we are doing and exacerbated by the growing use of algorithmic data matching and pattern finding.

2.4 To administer data well the UK government needs to support a consistent rights-based framework and mechanisms to realise children's rights and establish a social licence for data sharing between the child and family, and all of those with roles and responsibilities in each data process; educational settings, Local Authorities, the Department(s) for Education, companies, and other third-parties for consistent, confident data handling and to ensure safe, fair and lawful data processing also for the purposes of public interest research.

2.5 There is only **rarely a route for families' involvement in decisions that affect their child** from high level democratic discussion of the corporate reform of education through to the introduction of technology in education, down to the lack of consultation on the installation of CCTV collecting data via cameras and microphones, even in school bathrooms.

2.6 **Policy ignores the law today on fair processing.** Although the ICO audit of the Westminster Department for Education made 139 recommendations and was tasked with changes there is no new visible remedy for failing to tell people how their data is used, after collection from educational settings

2.7 Policy ignores the law today. The biggest driver of profiling children in the state education sector, despite data protection law stating in the GDPR about children that profiling children should not be routine, **is the Progress 8 measure**: about which Leckie & late Harvey Goldstein (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 have often been to date."[11]

2.8 Pigeon-holing children by design, and the creation of the 'datafied child'[12], its implications for the child and society are staggering. In the words of a former global education company CEO in 2012:

> ***"the human race is about to enter a totally data mined existence, and it's going to be really fun to watch...the world in 30 years is going to be unrecognisably data mined...education happens to be today, the world's most data mineable industry– by far."***
>
> Educational Platform Knewton (now Wiley) former-CEO, Jose Ferreira (2012)[13]

2.9 Core national education infrastructure must be put on the national risk register. Dependence on products such as Google for Education, MS Office 365, which are the route to providing the Department and government with pupil information, and cashless payment systems which function on the data in schools and ensure day-to-day running of schools, all need to have a further duty to transparency reporting obligations. We are currently operating in the dark where remote learning is and is not supportable, and about the implications of dependence on these systems for the delivery of key school functions and children's learning.

---

[11] Leckie, G., & Goldstein, H. (2016). *The evolution of school league tables in England 1992-2016: 'contextual value-added', 'expected progress' and 'progress 8'*. (Bristol Working Papers in Education Series; Vol. #2/2016). Graduate School of Education, University of Bristol. http://www.bristol.ac.uk/media-library/sites/education/documents/bristol-working-papers-in-education/The%20evolution%20of%20school%20league%20tables%20in%20England%201992-2016.pdf

[12] Lupton, D. and Williamson, B. Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, *19*(5), 780–794. https://doi.org/10.1177/1461444816686328

[13] Quotes source: YouTube channel of the Office of Educational Technology at the US Department of Education. https://www.youtube.com/watch?v=Lr7Z7ysDluQ Knewton, an adaptive learning company that has developed a platform to manage educational content, has developed courseware for higher education https://www.knewton.com/ It was bought by Wiley in 2019.

3. Protecting privacy and acting ethically: what people want

3.1 When it comes to a child's personal data being passed from a school to third parties or to the Department for Education (DfE), parents want to be asked for consent or exercise a right to object. Survation[14] asked 1,004 parents of state-educated children aged 5-18 on behalf of defenddigitalme, between 17th – 20th February 2018 about their understanding of which technologies are used, and how data are used. Most strongly parents 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. The Department cannot meet requests adequately.
- 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 may give out data from the National Pupil Database to third parties.

3.2 Current practice does not enable the exercise of rights, set out in UK domestic and other data protection law. The International Conference of Data Protection and Privacy Commissioners 2018, found that "Even where educational authorities have sufficient authority to engage and use e-learning platforms, individuals should have the right to opt out and receive educational services through alternative methods."[15]

3.3 Current practice goes beyond what parents expect and the boundaries of law about purpose limitation

"**Personal data shall be … collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')" (The GDPR, Article 5(1)(b))

3.4 "Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be **subject to appropriate safeguards**, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall **ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation**. Those measures may include

[14] The survey was commissioned as part of defendigitalme's work in a review of children's data privacy in education for The State of Data 2018. https://defenddigitalme.com/2018/03/only-half-of-parents-think-they-have-enough-control-of-their-childs-digital-footprint-in-school/

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

pseudonymisation provided that those purposes can be fulfilled in that manner. **Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner**." (The GDPR, Article 89(1))

3.5 A stronger foundation must be built first including data usage reports for children and families to know '*who knows what about me',* **Data privacy and protection must be introduced as part of basic teacher training and into compulsory CPD**, and regulation of current policy and practice as set out (2), should begin through consultation.

3.6 Professor Sonia Livingstone who recently carried out research funded by the ICO, reports that children want their profiles, such as on social media, wiped clean at 18. 'The children were generally mystified as to why tech companies were interested in personal information they saw as quickly going out of date as they grew up. She added: "*Creepy is a really common word that they use. It's creepy and sinister that all that data is being kept*." The same should be possible for their school records with history of behaviour and exclusions which even under the Rehabilitation of Offenders Act 1974 would be suppressed from distribution, but as non-criminal records, reasons for exclusion such as violence, sexual misconduct, or drugs may be passed on for life to third parties, without a child's (or their later adult) knowledge.

3.7 The DfE has relied on the organisation not *publishing* the pupil-level data to protect pupil confidentiality, but handed out identifying pupil data to press, charities and other third parties without small numbers suppression. This practice should be ended with support of statutory guidance or as part of legislation to create an umbrella act on Education and Digital Rights.[16]

4. Recommendations

4.1 The *national data strategy*[17] fails to take a rights based approach in its desire to '*unlock the power of data across government and the wider economy.*' While DCMS asks for views on trust on use, it has not sought to address rights around collection and retention. This prevailing attitude and approach contravenes the second principle of data protection law, purpose limitation as does the forthcoming Data Protection and Digital Information Bill.

4.2 Prioritise privacy in the rights of the child in the digital environment across the public sector by incorporating the Recommendation CM/Rec(2018)7 of the Council of Europe

[16] Defend Digital Me (2019) Manifesto for Education and digital rights and data (revision forthcoming 2024) https://defenddigitalme.org/wp-content/uploads/2019/11/defenddigitalme-manifesto-2020-for-digital-rights-in-education.pdf

[17] National Data Strategy open call for evidence (June 2019) https://www.gov.uk/government/publications/national-data-strategy-open-call-for-evidence/national-data-strategy-open-call-for-evidence#questions

Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment across the public sector.[18]

4.3 The government should ensure effective implementation of their obligations under Article 13 of the European Convention on Human Rights, and other international and human rights instruments, to fulfil a child's right to an effective remedy when their human rights and fundamental freedoms (such as Article 8) have been infringed in the digital environment.

4.4 We would welcome legislation, statutory Codes of Practice introduced into existing UK Data Protection law, and enforcement action to protect the full range of human rights of the child and young people in the digital environment in education.

4.5 The safeguards on national pupil data management should be of the highest standard across all of the four[19] UK national pupil databases, and use by third parties through release by government departments must become transparent and consensual.

4.6 Subject access rights should be standardised for children across all schools in the UK to change the inconsistency between Local Authority and academy/free school models of support of parental and child rights to subject access and access to the educational record and the wide variety of school information management systems (stored in schools or offsite on companies' cloud servers), platforms and apps in use.

4.7 Like the Partridge Review of health data (2014) an independent audit should take place of the commercial reuse of children's personal confidential data from national pupil data, distributed at national level to find out where it has gone and inform families.

4.8 Public Authorities should document and publish

- commercial processors and subprocessors engaged in children's data processing
- a register of any commercially obtained sources of personal data collected for processing, or linkage with data provided by individuals in the course of their public sector interactions, and update it on a regular basis. (i.e. Data brokers, third-party companies, social media)
- Data Protection Impact Assessments, Retention schedules, and GDPR s36(4) Assessments with periodic fixed review to address changes
- A register of all automated and AI supported algorithmic decision making tools

[18] Recommendation CM/Rec(2018)7 Guidelines to respect, protect and fulfil the rights of the child in the digital environment
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808b79f7

[19] A comparison of national pupil databases in the UK composed by defenddigitalme
http://defenddigitalme.com/wp-content/uploads/2018/03/UK_pupil_data_comparison-1.pdf

5. Limitations on exploitation and high risk technology, and research in school settings, appropriate to children

5.1 Consultation should be carried out on legislative limitations of surveillance in educational settings, via various biometrics, facial recognition and neuro-/cognitive technology by commercial companies, or via web cam, voice recording, or gait and movement analysis, noting UN Special Rapporteur David Kaye's call for a moratorium on facial recognition technology[20].

5.2 School social media tools must free pupils and students from any obligation of using personal profiles and accounts, and to avoid privacy risks, separate group and personal accounts, and more broadly, limit their use for school communications and administration.

5.3 Artificial intelligence companies should not exploit children's data gathered in the course of compulsory education, for their own company product development which is currently routine but unlawful data practice.

5.4 Behavioural science, neuroscience and other emerging technologies should not be trialled in schools. Any research studies in other edTech and interventions should require independent and published ethical oversight and opt in consent from parents and the child.

6. Historical data collections need enforcement for respect of human rights and data protection law

6.1 The state must address the requirements under the Data Protection Act 2018 (and GDPR Article 25[21]) to minimise its data collections and ensure proper policy, technical and security measures to address excessive data collection and enforce retention (including at national levels on leaving school), limit unique identifiers, and ensure anonymisation.

6.2 Children's data must not be used for purposes incompatible with the one that legitimised their collection and that the people were told about at that time. Non-educational purposes of national pupil data by other government departments (Home Office) must end.[22] Instead, the changing scope of data collected and discussion over reuse is moving towards more reuse without informed processing.

6.3 Explore a non-commercial-use duty on data collected prior to changes of law, and supporting communications about re-uses.

---

[20] Moratorium call on surveillance technology to end 'free-for-all' abuses: UN expert
, (June 2019) David Kaye recommendations, United Nations Special Rapporteur on freedom of opinion and expressionhttps://news.un.org/en/story/2019/06/1041231

[21] ICO Data Protection by Design and Default (Article 25) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

[22] Timeline of Home Office access to pupil data in England for immigration enforcement purposes https://defenddigitalme.com/timeline-school-census/

6.4 It is common for edTech to re-use personal data provided for the school / pupil's purposes of direct admin, teaching or communications,, for their own commercial company purposes; whether for in-app advertising, pitching at parents' emails for upgraded or sister products, or product development including new AI tools; chat bots, and virtual learning platforms. Children, young people and their parents being the captive addressees of marketing is a consumer protection problem. But from the human rights point of view, it is the prior collection of personal data, in order to send the data subjects marketing messages later, and its further repurposing for indirect uses, which is problematic for privacy.

7. Procurement must respect international law and guidelines regarding the impact of the business sector on children's rights

7.1 **The UN General comment No. 16 (2013) on State obligations states** *"a State should not engage in, support or condone abuses of children's rights when it has a business role itself or conducts business with private enterprises. For example, States must take steps to ensure that public procurement contracts are awarded to bidders that are committed to respecting children's rights. State agencies and institutions, including security forces, should not collaborate with or condone the infringement of the rights of the child by third parties.* ***States should not invest public finances and other resources in business activities that violate children's rights****."*

7.2 The European High Level Expert Working Group on Artificial Intelligence (HLEG-AI) reported on policy and business in June 2019, and proposed that children should be better protected when used with such technologies.

> "*Children should be ensured a free unmonitored space of development and upon moving into adulthood should be provided with a "clean slate" of any public or private storage of data related to them*." [23] **(Policy and Investment Recommendations for Trustworthy Artificial Intelligence, HLEG on AI, June 2019)**

8. High risk datasets

8.1 There are current practices in national pupil data management that we consider high risk and that require urgent change.

8.2 The DfE receives the sexual orientation and religious affiliation of individuals from JISC (formally HESA) and retains them on students' named longitudinal education records indefinitely.

As of February 2023, the DfE held the self-declared sexual orientation of 3,213,683 individuals in the National Pupil Database (in a total of around 23 million records) and the religious affiliation of 3,572,489 people, all on their named records.[24]

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

8.3 Oversight or public record of data transactions are both lacking.The law was changed[25] through the Higher Education and Research Act 2017 and subsequent regulations, to enable distribution for a wide range of purposes including to commercial companies. Neither the OfS nor HESA publish any register of their distribution of student data, and HESA is not subject to Freedom of Information law.

8.4 The Secretary of State should consult with stakeholders in the Higher Education sector, before introducing regulations to end the current distribution of named and identifying students' sexual orientation, religion, and disability beyond the point of collection and beyond internal use at the Higher Education institution. It would replace the current passing around of named data and require current policy to be replaced by sharing only statistics with the Office for Students, HESA, JISC, Funding bodies, and passed on for retention in the National Pupil Database at the Department for Education.

8.5 In 2023, we have asked a sample of 30 Universities across Scotland, England and Wales, and only one has carried out any Data Protection Impact Assessment. It found risk of harm and threat to life. Download the summary[26] and links to FOI in Scotland and England and Wales.

8.6 In our view, national records of children in need of child protection are inadequately shielded.

The CIN census[27] is a statutory social care data return made by every LA to the DfE, it captures information about all children who have been referred to children's social care regardless of whether further action is taken. As of 8 September 2022, there were only 70 individuals flagged for shielding and that includes both current and former pupils. There were 23 shielded pupil records collected by the Department via the 2022 January censuses (covering early years, schools and alternative provision).

8.7 No statement or guidance is given directly to settings about excluding children from returns to the DfE. As of September 2022, there were 2,538,656 distinct CiN (any child

---

[24] The Department for Education FOI https://www.whatdotheyknow.com/request/pupil_data_religion_and_sexual_o#incoming-2262183

[25] Higher Education and Reserch Act 2017 and Regulations 2018/19 https://www.parliament.uk/documents/lords-committees/Secondary-Legislation-Scrutiny-Committee/Session%202017-19/Product%20safety/Defenddigitalme%20submission%20on%20%20Higher%20Education%20Act%20Regulation%202019%20v2.pdf

[26] Defend Digital Me (2023) Does your national school record reveal your sexual orientation or religion? https://defenddigitalme.org/2023/04/02/does-your-national-school-record-reveal-your-sexual-orientation/

[27]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066288/Children_looked_after_by_local_authorities_in_England_-_guide_to_the_SSDA903_collection_1_April_2021_to_31_March_2022.pdf

referred to children's social care services within the year) / LAC child records (going back to 2006), regardless of at-risk status, able to be matched to some home address information via other (non CiN / LAC) sources included in the NPD.[28] Data is highly sensitive and detailed, including “categories of abuse”

9. Horizon scanning

9.1 We are concerned that the austerity agenda comes at the cost of students’ privacy. The cuts to Jisc funding by the Department for Education, came at the same time as Jisc is seeking to exploit data assets of 6m students, which it can repackage to others. In a March 2018 statement online applicable to HE and FE in England, the CEO wrote[29],

> *“Due to a fundamental shift in our funding model, over a five year period the Government has reduced our budget by more than £10m. DfE has asked us to work...on introducing a subscription from August 2019. To minimise the subscription as much as possible, Jisc is absorbing more than £4 million of income reduction.”*

9.2 The former Universities Minister Mr Sam Gyimah confirmed in a parliamentary question[30] about the change of law to allow commercial third party organisations the Office for Students (OfS) to pass data on, that it, *“does not place limitations on types of information that may be provided [to third parties], and therefore could include personal data.”*

9.3 Do we all want to be turned into training datasets for AI without our permission or being told? That's what we at Defend Digital Me believe the new UK Data Protection and Digital Information Bill is setting us up for. For children it could mean a lifetime of direct marketing, political profiling, and data given away as a child they can no longer control using data protection law, once they have capacity.

9.4 The DfE certainly seems to be already thinking about using pupil data for AI development as Schools Week (June 2023) reported: "Barran said ministers were asking “a number of questions”, including on ownership of the [pupil] data and “what’s it worth”.

9.5 Defend Digital Me commissioned an independent Legal Opinion by Stephen Cragg KC of Doughty Street Chambers relating to the Data Protection and Digital Information Bill (2023).

---

[28] https://www.whatdotheyknow.com/request/pupil_data_children_at_risk_data#incoming-2134108

[29] Paul Feldman CEO, Jisc, March 2018 statement online https://www.jisc.ac.uk/membership/further-education-subscription

[30] PQ 156350 (June 21, 2018) Mr Sam Gyimah To ask the Secretary of State for Education, whether confidential personal information relating to (a) Higher Education personnel and (b) students may be provided by the Office for Students to (i) Pearson Limited, (ii) the HMRC, (iii) student loans company and (iv) other persons prescribed the Higher Education and Research Act 2017 (Information Sharing) https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2018-06-21/156350/

https://defenddigitalme.org/2023/11/28/new-legal-opinion-on-the-data-protection-and-digital-information-bill/

9.6 The Data Protection and Digital Information Bill (at the time of writing at the end of 2023) takes the UK in the wrong direction if we are to ensure safe, fair, transparent use of people's data in the modern world. We must reconcile the focus of the UK national data strategy, with a human rights-based governance framework to move forward the conversation in ways that work for the economy and research, and with the human flourishing of our future generations at its heart.

9.7 Defend Digital Me is calling for this Bill to be withdrawn, and instead an ICO Code of Practice to be drafted for (existing) Data Protection law in Educational Settings. This should be in line with the **Council of Europe: Guidelines on children's data protection in education (2021).**[31]

10. Public engagement evidence of public attitudes towards data

---

10.1 Our own engagement work has focussed with a youth group aged 14-25 and at a small scale. Published in 2020 in our work, *The Words We Use in Data Policy: Putting People Back in the Picture*, reflected what the Office for the Regulation of National Statistics then went to publish in their own 2022 report, **Visibility**, **Vulnerability** and **Voice** (as a framework to explore whether the current statistics are helping society to understand the experiences of children and young people in all aspects of their lives). Young people worry about misrepresentation, about the data being used in place of conversations about them to take decisions that affect their lives, and about the power imbalance it creates without practical routes for complaint or redress. We all agree children's voice is left out of the debate on data about them.

10.2 A wide range of publications are available from over a decade of public engagement. All find similar views. There is public trust in public interest research but people want to have a say and control with whom any personal data is shared for any purposes beyond direct care and the point of collection:

- RAENG (2010) On children and health data Privacy and Prejudice: young people's views on the development and use of Electronic Patient Records (911.18 KB). They are very clear about wanting to keep their medical details under their own control and away from the 'wrong hands' which includes potential employers, commercial companies and parents.

[31] Council of Europe (2021) Guidelines for Children's data protection in an education setting. Jen Persson, Director of Digital Me was the Subject Matter Expert and supported the CoE Committee on Convention 108 in the drafting https://edoc.coe.int/en/children-and-the-internet/9620-childrens-data-protection-in-an-education-setting-guidelines.html

- ADRN (2013) on *deidentified* personal data including red lines in the "Dialogues on Data" report on creating mega databases and commercial re-use
- **The Royal Statistical Society (RSS) (2014) https://www.ipsos.com/ipsos-mori/en-uk/new-research-finds-data-trust-deficit-lessons-policymakers The data trust deficit with lessons for policymakers
- UCAS applicant survey with 37,000 respondents (2015) https://www.ucas.com/corporate/news-and-key-documents/news/37000-students-respond-ucas%E2%80%99-applicant-data-survey A majority of UCAS applicants (64%) agree that sharing personal data can benefit them and support research into university admissions, but they want to stay firmly in control, with nine out of ten saying they should be asked first.
- Wellcome Trust/ Ipsos MORI (2017) The One-Way Mirror: Public attitudes to commercial access to health data https://wellcome.figshare.com/articles/journal%20contribution/The_One-Way_Mirror_Public_attitudes_to_commercial_access_to_health_data/5616448/1
- defenddigitalme (2018) Parents' poll 'Only half of parents think they have enough control of children's digital footprint'. https://defenddigitalme.org/2018/03/only-half-of-parents-think-they-have-enough-control-of-their-childs-digital-footprint-in-school/
- DotEveryone(2018-20) https://doteveryone.org.uk/project/peoplepowertech/ Their public attitudes report found that although people's digital understanding has grown, that's not helping them to shape their online experiences in line with their own wishes.
- LSE (2019-20) Children's privacy online https://lse.ac.uk/my-privacy-uk

10.3 Defend Digital Me edTech and pupil data Briefing: November 2023 (WIP) v.1.8 for the debate in the House of Lords https://defenddigitalme.org/wp-content/uploads/2023/11/Defend-Digital-Me-edTech-and-pupil-data-Briefing-November-2023-v1.8.pdf

10.4 2022 House of Lords Children's Private Information: Data Protection Law Volume 826: debated on Monday 12 December 2022 https://hansard.parliament.uk/Lords/2022-12-12/debates/225551A8-EA02-4D2B-B2F2-6692BD174935/Children%E2%80%99SPrivateInformationDataProtectionLaw

10.5 Previous evidence to the Justice and Home Affairs Committee

We provided evidence to the Justice and Home Affairs Committee Inquiry on New technologies, data, and the application of the law in 2021 https://defenddigitalme.org/wp-content/uploads/2021/11/Submission-to-the-Justice-and-Home-Affairs-Committee-Inquiry-New-technologies-and-the-application-of-the-law-defend-digital-me.pdf

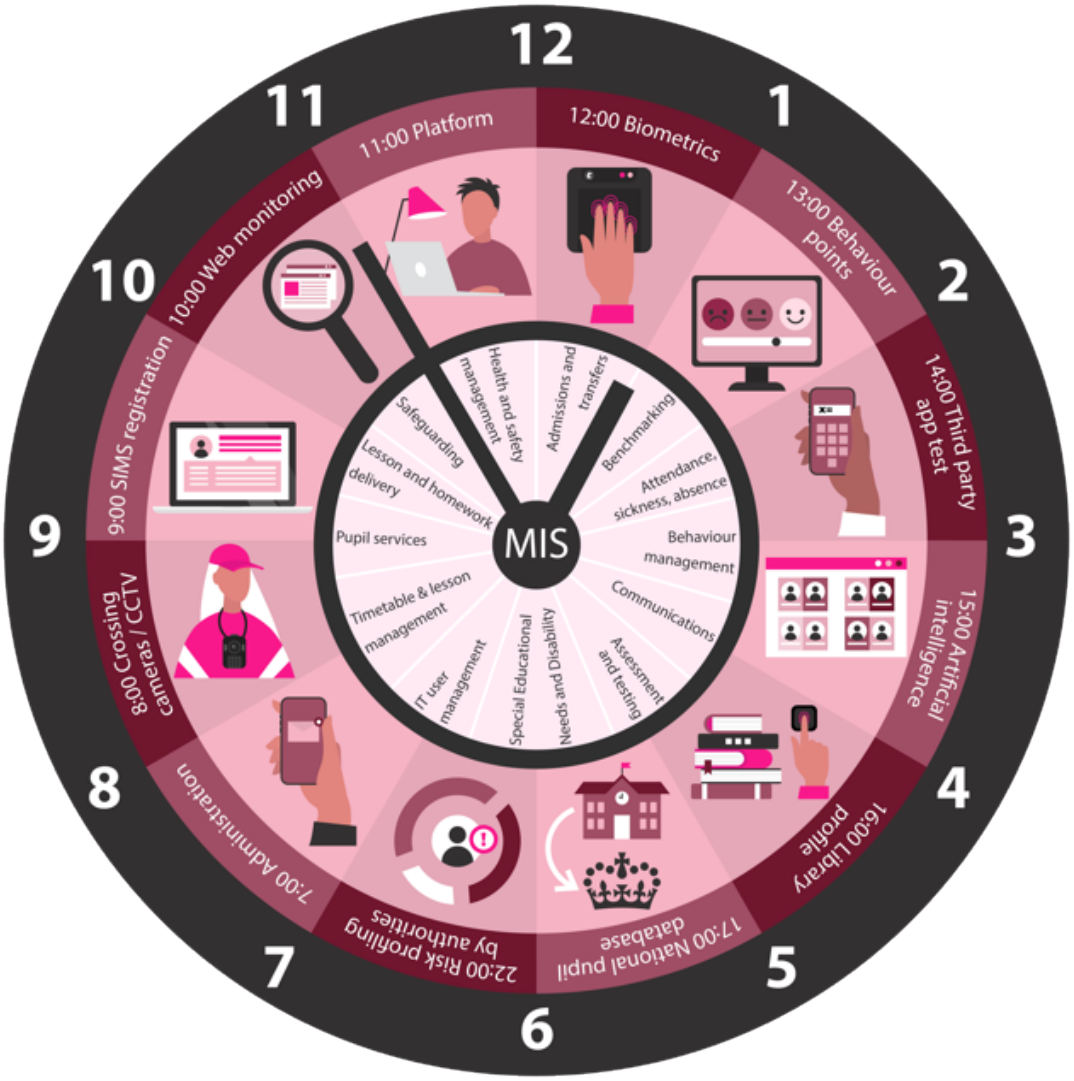
10.6 In our report **The Words We Use in Data Policy: Putting People Back in the Picture (2021)** we explore why and how the language used about data in public conversations does not work. We suggest what must change to better include children for the sustainable

future of the UK national data strategy. https://defenddigitalme.org/research/words-data-policy/

We have published various other research and reports to support the improvement of how the data landscape is seen and understood, how the narratives are spoken, and increase policy makers knowledge of the digital landscape in state education. https://defenddigitalme.org/research/

10.7 There is a significant opportunity to simplify data laws in education through review and revision of the sprawling range of data collection primary and enormous expansions carried out only through secondary legislation since 1996.

11. A day-in-the-life of a datafied child in state education



11.1 From before breakfast to bedtime and beyond, a pupil's personal data are collected and may be transferred to hundreds of third parties in one day and thousands across their lifetime education. For school administration and central information management systems, and for communications, and use by local and national pupil databases. By apps, platforms, cashless payment systems, including biometrics, special educational needs and disability, and health data. On behavioural platforms, in exams and tests (state mandated and with a wide range of commercial test suppliers), in safeguarding software, seating plans, borrowing library books, and at after-school clubs. On CCTV, classroom cameras, lesson capture tools, and classroom and patrol bodycams. And even at home, for their homework, logged into school accounts, and around the clock. The types of data being collected are increasingly biometric and bodily data from behaviour and thought and claims to be able to process mood and emotion and to "keep children on point".

11.2 There is no way for a child to understand or track their digital footprint by the time they are 18, or have any ability to reclaim control over it by the time they leave state education. There is a great opportunity to change this and it is an urgent task for good data governance over the next decade.

We are happy to answer any questions the Committee may have.
Defend Digital Me, 2023

About defenddigitalme

Defend Digital Me is a call to action and non-partisan civil society organisation. We campaign for safe, transparent and fair use of personal confidential data across the education sector in England. We are funded wholly by non-commercial interests through philanthropic grants (most recently from the Joseph Rowntree Charitable Trust). Registered company number 11831192 | ICO registration number ZA499530

Director and Founder of Defend Digital Me, Jen Persson held a two-year lay role on the ESRC funded UK Administrative Data Research Network (ADRN) 2015-17 Approvals Panel to assess research requests (https://tinyurl.com/adrn2015) and in 2023 is a Subject Matter Expert for the Council of Europe Digital Citizenship Directorate and member of the Council of Europe AI and Education working group. She is a former Subject Matter Expert for the Council of Europe Committee on Convention 108+ on data protection in educational settings 2019-20 and supported drafting of Data Protection Guidelines adopted in November 2020.[32]

[32] Council of Europe Committee on Convention 108 Guidelines on data protection in an educational setting (2020) https://www.coe.int/en/web/data-protection/-/protect-children-s-personal-data-in-education-setting-

January 2024