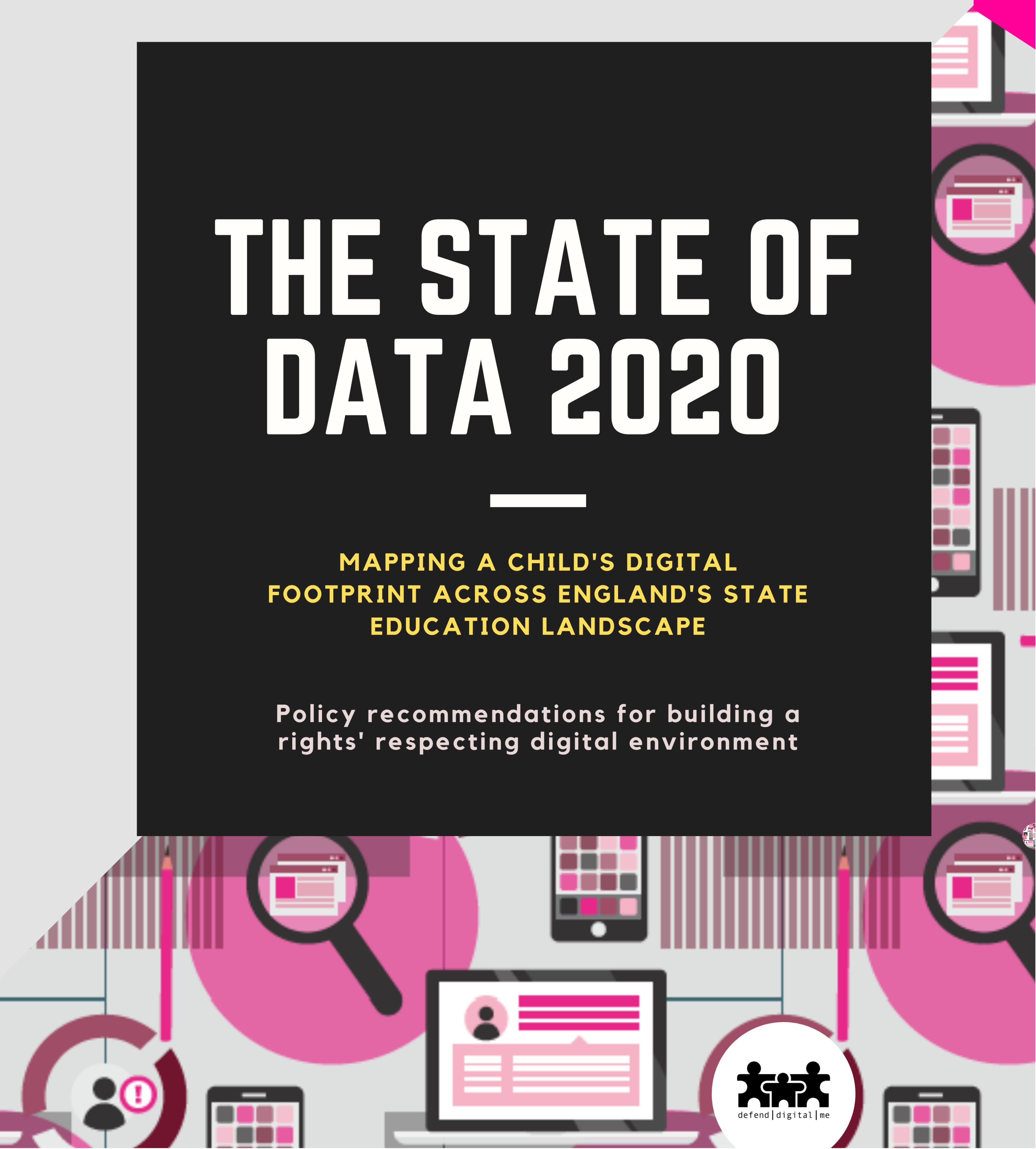
defend|digital|me

THE STATE OF DATA 2020

MAPPING A CHILD'S DIGITAL FOOTPRINT ACROSS ENGLAND'S STATE EDUCATION LANDSCAPE

Policy recommendations for building a rights' respecting digital environment



defend|digital|me

The State of Data 2020: Part 1 of 5

October 2020
v.2.2

About defenddigitalme and what we do

We are a non partisan civil society organisation. We campaign for safe, transparent and fair use of personal confidential data across the education sector in England. Funded by the Joseph Rowntree Reform Trust.

defenddigitalme l Registered company number 11831192 l ICO registration number ZA499530
defenddigitalme.org l email info@defenddigitalme.org

citation l The State of Data 2020 report: mapping children's data in state education in England (2020) defenddigitalme https://defenddigitalme.org/the-state-of-data-2020/ part 1

This is the State of Data Report part 1 of 5 parts. The complete report can be found online at https://defenddigitalme.org/the-state-of-data-2020/

Contents

Foreword

The State of Data Report provides a snapshot of the uses and abuses of children's data in school. Its rich findings will be of great help in tackling the inequities and intrusions that children suffer.

Robust data privacy protections in schools and educational settings are urgently needed. School is not optional for children and therefore the harvesting of their data must not be compulsory.

A child's gait, their visits to the bathroom, their exam results, their parents' immigration status and their visits to the school counsellors must not be available to third parties, nor should companies be allowed to claim educational benefits that are unproven nor be able to impact on young people's educational outcomes without meeting minimum standards that ensure their products are fit for use.

This comprehensive report deserves close reading by all those concerned with children's privacy and security. Ministers and officials in the Department of Education and government would do well to consider its detailed recommendations that reveal both a gross injustice for an entire generation of children, and usefully signpost the way forward.

Baroness Beeban Kidron, Chair
5Rights Foundation

Executive summary

Children have lost control of their digital footprint by their fifth birthday simply by going to school.

The State of Data 2020 report

- is a call to action from teachers, parents and young people for change in law, policy and practice on data and digital rights in state education and its supporting infrastructure
- maps the scope of every statutory data collection for the first time, from the Early Years to A-levels in attainment tests and the censuses collected by the Department for Education
- reveals gaps in oversight, transparency and accountability in product trials and edTech that collect children's data; in what, why, and how it is used, through a selection of case studies

Data protection law alone is inadequate to protect children's rights and freedoms across the state education sector in England. Research trials are carried out routinely in classrooms without explicit parental consent and no opt-out of the intervention. Products marketed for pupils are increasingly invasive.[1] Students are forced to use remote invigilation tools that treat everyone as suspicious, with automated operations that fail to account for human differences, or that harm human dignity.[2]

This report asks government, policy and decision makers to recognise the harms that poor practice has on young people's lives and to take action to build the needed infrastructure to realise the vision of a rights' respecting environment in the digital landscape of state education in England.

We make recommendations on ten topics

1. Legislation and statutory duties
2. Assessment, Attainment, Accountability and Profiling
3. Administrative data collections and national datasets
4. Principles and practice using technology today
5. EdTech evidence, efficacy, and export intentions
6. Children's rights in a digital environment
7. Local data processing
8. Higher Education
9. Research
10. Enforcement

Now is a critical moment for national decision makers if they are serious about the aims of the National Data Strategy[3] to empower individuals to control how their data is used. After the damning 2020 ICO audit[4] of national pupil data handling at the Department for Education, will you make the changes needed to build better: safe, trustworthy public datasets with the mechanisms that enable children and families to realise their rights or will you stick with more of the same; data breaches[5] and boycotts[6] and bust opportunity?

[1] Staufenberg, J. (2019) Schools Week | New headsets monitor pupils' brain waves to track concentration https://schoolsweek.co.uk/new-headsets-monitor-pupils-brain-waves-to-track-concentration/

[2] Online law students 'had to use bucket toilet' in exams (2020) BBC https://www.bbc.co.uk/news/uk-england-53765462

[3] National Data Strategy (Sept.2020) https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

[4] ICO (2020) Statement on the outcome of the ICO's compulsory audit of the Department for Education https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/statement-on-the-outcome-of-the-ico-s-compulsory-audit-of-the-department-for-education/

[5] Trandall, S. (2020) Civil Service World | DfE data protection 'tightened significantly' after massive breach of learner records https://www.civilserviceworld.com/news/article/dfe-data-protection-tightened-significantly-after-massive-breach-of-learner-records

[6] Staton, B. (2017) Sky News | School census boycott over child deportation fear https://news.sky.com/story/school-census-boycott-over-child-deportation-fear-11067557 and The Times (2010) Thousands of Key Stage tests cancelled after teachers boycott exams https://www.thetimes.co.uk/article/thousands-of-key-stage-tests-cancelled-after-teachers-boycott-exams-qhlrvtqrb7t

Will you act to safeguard the infrastructure and delivery of state education and our future sovereign ability to afford, control, and shape it, or drive the UK state to ever more dependence on Silicon Valley and Chinese edTech, proprietary infrastructure on which the delivery of education relies today.

The 2020 exam awarding process demonstrated the potential for discrimination in data, across historical datasets and in algorithmic decision making. While some may consider the middle of a global pandemic is not the best time to restructure school assessment, progress and accountability measures, change is inevitable since some collections were canceled under COVID-19. Now is the time to pause and get it right. We are also at a decisive moment for many schools to decide if, or which new technology to invest in, now that most of the COVID-19 free-trial offers are over.

Privacy isn't only a tool to protect children's lives, their human dignity and their future selves. The controls on companies' access to children's data, is what controls the knowledge companies get about the UK delivery of education and the state education sector. That business intelligence is produced today by the public sector teachers and children who spend time administering and working in the digital systems. So while many companies offer their systems for free or at low cost to schools, schools have intangible costs in staff workload and support time, and donate those labour costs to companies for free. Our children are creating a resource that for-profit companies gain from.

Exclusive Department for Education funding to support schools' adoption of tech giants'[7] products in lockdown, further established their market dominance, and without any transparency of their future business plans or intentions or assurances over service provision and long-term sustainability.

The lasting effects of the COVID-19 crisis on children's education and the future of our communities, will be as diverse as their experiences across different schools, staff, and family life. Worries over the attainment gap as a result of lost classroom hours, often ignores the damaging effects on some children of the digital divide, deprivation and discrimination and lack of school places for children with SEND, that also affected children unfairly before the coronavirus crisis. Solutions for these systemic social problems should not be short term COVID-19 reactions, but long term responses and must include the political will to solve child poverty. Children's digital rights are quick to be forgotten in a rapid response to remote learning needs, but the effects on their digital footprint and lived experience might last a lifetime.

We call for urgent government action in response to the COVID-19 crisis and rapid digital expansions:

- the Department for Education to place a moratorium on the school accountability system and league tables as pupil data continue to be affected by COVID-19, making comparable outcomes and competitive measures meaningless and misleading. We suggest a pause on the Early Years attainment profile, and Key Stage One SATs and only sampling Phonics Tests and a sample of Key Stage Two SATS. Reception Baseline Test is not fit for purpose and should be stopped indefinitely, alongside the Multiplications Times Tables Check.
- core national education infrastructure delivered by the private sector should be put on the national risk register as its fragility has been demonstrated in the COVID-19 crisis
- publish a list of actions the Department will undertake in response to the 2020 ICO audit
- build better infrastructure at national, regional and local levels founded upon a UK Education and Digital Rights Act, and give it independent oversight through an ombudsman and champion of children's rights for national data in education, placed on a statutory footing.

[7] DfE press release (April 2020) Schools to benefit from education partnership with tech giants | Thousands of schools to receive technical support to start using Google and Microsoft's education platforms https://www.gov.uk/government/news/schools-to-benefit-from-education-partnership-with-tech-giants

Sector-wide attention and longer term action are needed to address

1. **Access and inclusion:** Accessibility design standards and Internet access and funding
2. **Data cycle control, accountability and security:** mechanisms are needed by industry and schools for lifetime governance and data management for where 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 product development and SME growth
6. **Lifetime effects of data on the developing child**: Permanency of the single pupil record
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 foreign-based edTech with implications for data export management, and increasing transparency over future costs, practice, and ensuring long-term stability for the public sector.

This year marks 150 years since the Elementary Education Act 1870 received royal assent. It was responsible for setting the framework for schooling of all children between the ages of 5 and 13 in England and Wales.

Todays' legislation, the Education Act 1996 is the primary legislation upon which most statutory instruments are hung to expand pupil data collections, and start new ones for millions of children generally as negative statutory instruments without public consultation or parliamentary scrutiny.

It is no longer fit for purpose and lacks the necessary framework when it comes to data processing and related activity in the digital environment in education. It is therefore our first in ten areas of recommended actions on the changes our children need.

1.1. Introduction

In 2020 as the world's children continue to be affected by school closures in the COVID-19 pandemic, technology plays a vital role in education. Some tools enable the delivery of essential information, connecting school communities outside the classroom. Others provide national platforms for sharing educational materials, or offer alternative means and modes of Assistive Technology and augmented communications, supporting the rights of those with disabilities.

But many families across the UK still don't have the necessary hardware or Internet access to support online remote learning at home. In addition, a lot of the critical infrastructure to deliver the administrative access to education is enabled by Silicon Valley big tech — companies originally set up by and for business, not educators. The Department for Education's (DfE) rapid response to a need for remote learning in the COVID-19 pandemic, bolstered the near duopoly in England's school system by offering funding in the Platform Provisioning Programme, to schools to get started with only two providers' systems— either Google or Microsoft.[8] Is that lack of sovereignty in the state sector sustainable? What is the current business model? What happens when freeware business models change? There is inadequate capability and capacity in schools to understand much of the technology marketed at them. Staff are expected to make quick and effective procurement choices for which they have often little training and can lack access to the necessary expertise.

Some of the greatest ongoing debates in the education sector on assessment and accountability, funding, curriculum and governance all have implications for children's digital records. And we are at an acute point of heightened awareness of disadvantage and distance learning. Understanding how technology should support these needs was part of the regular delivery of education. A large part of products offered to schools was for administrative support, but tools supporting learning to date have in the main offered stand-alone and closed commercial product offerings. The exceptional demands of remote learning now demand more focussed attention on what is desirable, not only on what is currently available.

Creating better public sector infrastructure and local systems

Today, schools overstretched by austerity, routinely push costs back to equally cash strapped parents. Lack of investment in school infrastructure means parents are increasingly asked to pay upwards of £400 in lease-to-buy hardware schemes and take on ever more back-office pupil admin through linked pupil-parental apps. Freeware products may choose to make money through data mining or ads instead of charging an upfront fee that schools can't afford. Children using the product may not know their data and behavioural activity is used as a free resource by companies in product development and research. Practice that can fail to comply with the law.[9]

Imagine instead, a fair and open market in which safe tools were supported that were effective, equitable, and proven to meet high standards. To support better accessibility, pedagogy and provide trustworthy emerging technologies we must raise standards and hold businesses and the state accountable for their designs and decision making.

Imagine if the government invested a flat rate in COVID-19 teacher training support, and open funding to build tools that schools need, to support a blended approach beyond autumn 2020.

[8] Schools to benefit from education partnership with tech giants (2020) Department for Education press release https://www.gov.uk/government/news/schools-to-benefit-from-education-partnership-with-tech-giants The Key: Digital education platform hub https://schoolleaders.thekeysupport.com/covid-19/deliver-remote-learning/make-tech-work-you/digital-education-platform-hub/

[9] Denham, E. The Information Commissioner (2017) Findings on Google DeepMind and Royal Free https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/

Imagine moving away from systems that siphon off personal data and all the knowledge about the state education system—using teachers' time and work invested in using the product for their own benefit—and instead the adoption of technology focussed on children's needs and transparently benefited the public interest. Imagine decentralised, digital tools that worked together across a child's school day centred on the child's education rather than a series of administrative tools that are rarely interoperable and most often siloed.

Despite the best intentions of peer-to-peer demonstrator schools to share best practice and selected digital products, there is no joined-up vision for a whole curriculum approach, underpinned by pedagogy and proven child outcomes. Promotion encourages adoption of ABC products because it can help you with XYZ as a bolt-on to current practice. Rather than looking at a child-centric and teacher-centric experience of teaching and learning and asking what is needed. While many products look and sound appealing, many of the learning outcomes are contentious and unproven, and are rarely compared with giving every secondary school child a full set of subject text books for example.

Government must work to safeguard the national infrastructure behind the delivery of state education and our future state ability to afford, control, and shape it. But it must also provide a high standards framework for educational settings to be able to address the lack of equity and access at local level; due diligence in procurement in technical, company integrity and ethical terms.

There is 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 in school bathrooms. Without new infrastructure, the sector has no route to move forwards to develop a consistent social contract to enable and enforce expectations between schools and families.

Creating safe national data systems

Learners have also found themselves at the sharp end of damaging algorithms and flawed human choices this summer across the UK, as the exam awarding processes 2020 left thousands of students without their expected grades and stepping stone to access university. People suddenly saw that a cap on aspiration[10] was a political choice, not a reflection of ability.

The historic data used in such data models is largely opaque to the people it is about. The majority of parents we polled in 2018 do not know the National Pupil Database exists at all. We have campaigned since 2015 for changes to its management; transparency, security and reuses.

In the wake of the national Learning Records Service breach,[11] the Department for Education tightened access to the approval process for new users of the 28 million individuals' records in Spring 2020. The Department now requires firms to provide details of their registration with both the Information Commissioner's Office and Companies House, as well as evidence of their being a going concern. And it will be dependent on firms providing "a detailed description of why they need access" —all of which one would have expected to be in place and that routine audit processes would have identified before it was drawn to national attention by the Sunday Times[12].
But it is just one of over 50 such databases the Department for Education controls, and what about the rest? The ICO findings from its 2020 audit should be applied to all national pupil data.

These databases are created from data collected in the attainment tests and school censuses, some of which didn't happen this year. So what needs to happen next?

[10] Mcinerney, L. (2020) The Guardian | England's exam system is broken – let's never put it together again https://www.theguardian.com/education/2020/sep/15/englands-exam-system-is-broken-lets-never-put-it-together-again

[11] Trandall, S. (2020) Civil Service World | DfE data protection 'tightened significantly' after massive breach of learner records https://www.civilserviceworld.com/news/article/dfe-data-protection-tightened-significantly-after-massive-breach-of-learner-records

[12] Bryan, K. et al (2020) Sunday Times | Revealed: betting firms use schools data on 28m children https://www.thetimes.co.uk/article/revealed-betting-firms-use-schools-data-on-28m-children-dn37nwgd5

After the exams fiasco 2020, and pause on attainment testing for the accountability system, we propose a moratorium on league tables, accountability, and Progress 8 measures until at least 2025. Delay the national central collection of children's records and scores in the new Reception Baseline and Multiplications Times Tables Tests. Data should work to support first and foremost the staff that create it in the direct care of the children in front of them. The Department for Education should receive sampled data from Early Years, Phonics and Key Stage Two testing and enable a decentralised model for the minimum necessary information transfers of Year 6 into Year 7 transition, which may adjust the Common Transfer File.

Building a rights' respecting digital environment in education

Few families would let an unlimited number of strangers walk into their home, watch what they do on-screen, hear what they say or scan every Internet search and label it with risk factors. No one would let strangers or even school staff take a webcam photo of their child without their knowledge or permission. We would not expect outsiders who were not qualified educators to stand in the classroom and nudge a child's behaviour or affect their learning without DBS checks, safety and ethical oversight and parents being informed. Yet this is what happens through current technology in use today, across UK schools.

Imagine England's school system as a giant organisational chart. What do you see? Which institutions does a child physically pass through? 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 education and long after they leave school.

Learners' rights are rarely prioritised and the direction of travel is towards ever more centralised surveillance in edTech, more automated decision making and reduced human dignity and may breach data protection, equality and consumer law.[13] The need for protection goes beyond the scope of data protection law and to the protection of children's right to fundamental rights and freedoms; privacy, reputation, and a full and free development.

"The world in thirty years is going to be unrecognizably datamined and it's going to be really fun to watch," said then CEO of Knewton, Jose Ferreira at the White House US Datapalooza in 2012.[14] *"Education happens to be the most data mineable industry by far.*"

We must build a system fit to manage that safely and 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.[15]

We must also enable children to go to school without being subject to commercial or state interference. "*Children do not lose their human rights by virtue of passing through the school gates… Education must be provided in a way that respects the inherent dignity of the child and enables the child to express his or her views freely*..."[16]

[13] Perry, J. (2020) Why online exams may breach data protection, equality and consumer law https://www.monckton.com/why-online-exams-may-breach-data-protection-equality-and-consumer-law/

[14] José Ferreira (2012) Knewton CEO | Education Datapalooza https://www.youtube.com/watch?v=Lr7Z7ysDluQ

[15] Statistics: Longitudinal Educational Outcomes (LEO) higher education graduate employment and earnings (At the time of writing last update June 2020) https://www.gov.uk/government/collections/statistics-higher-education-graduate-employment-and-earnings

[16] The UN Convention Committee on the Rights of the Child (2001) paragraph 8 of its general comment No.1 on the aims of education https://www.ohchr.org/EN/Issues/Education/Training/Compilation/Pages/a) General CommentNo1TheAimsofEducation(article29)(2001).aspx

The Convention on the Rights of the Child makes clear that children have a specific right to privacy. Tracking the language of the UDHR and ICCPR, Article 16 of the Convention states that "*no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation*," and reaffirms that "*the child has the right to the protection of the law against such interference or attacks. These standards imply that children should be given the same levels of protection for their right to privacy as adults. When contextualising children's right to privacy in the full range of their other rights, best interests, and evolving capacities however, it becomes evident that children's privacy differs both in scope and application from adults' privacy*." (UNICEF, 2017)[17]

By placing this background work into the public domain (in parts two to five of this report) we intend it for others to use and help keep it up to date with current information and case studies in the constantly evolving areas of statutory data collections and technology to collectively build better.

1.2 Scope of the report

We set out to map a snapshot of the current state of data processing in 2020 for children in education in England, age 2-19. In Parts 2-4 we describe a selection of some of the common data processing, what systems do and why, how they share data and consider their risks.

This report is about how systems create, use and exploit information collected *about children* as well as content created *by them*, and how that data is processed by third-parties, often for profit, generally at public sector cost in terms of school staff time and from school budgets.

We include applied case studies in the online report content (Part 3), brought to our attention by a wide range of stakeholders including young people, parents, state school, private school and public authority staff with the aim of drawing out more concrete discussion of common issues in a rapidly changing field. We are grateful to the companies that contributed to our understanding of their products and reviewed the case studies in advance of publication.

We do not attempt to present this as a comprehensive view of the entire education landscape that is constantly evolving. We need to do further research to map data flows for children with special educational needs who leave mainstream schooling and 'managed moves'. We do not cover secure children's homes or secure training centres. But there are consistent gaps with regard to lack of respect for child rights highlighted across Ofsted reports of all settings where children receive education, so that children in the Oakhill Secure Training Centre[18] may have much in common with those in edTech demonstrator schools.

We have sought views from discussion with a wide range of others: academics, benchmarking companies, data protection officers, data consultancies, researchers, school network managers, suppliers, vendors. In 2019 we also ran workshops with young people.

We include the opinions of over 1,000 parents in a poll we commissioned through Survation in 2018, and the views from 35 school IT network managers and staff on the online forum Edugeek, polled just before the GDPR came into enforceable effect in May 2018. The latter was too small to be a representative sample of opinions, but is an interesting snapshot of views in time.

[17] Unicef quote taken from the 2017 Discussion paper series: Children's Rights and Business in a Digital World: Privacy, protection of personal information and reputation https://www.unicef.org/csr/paper-series.html

[18] An inspection of Oakhill Secure Training Centre undertaken jointly with Ofsted (2019) https://www.justiceinspectorates.gov.uk/hmiprisons/inspections/oakhill-secure-training-centre-8/

This report is not about how children access or use the Internet in their personal lives. There is already a lot of discussion about child protection with regard to online stranger-danger, or restricting their access to harmful content.

We aim to map what personal data is collected by whom, for what purposes and where it goes and why. This report is only a sample of the everyday data collection from children in the course of their education and tells only some of the story that we can see. The fact that so much is hidden or hard to find is of itself a key concern. Gaps that readers familiar with the sector may identify, may highlight how hard it is for families to understand the whole system. We intend to update this knowledge base in an online repository and maintain it with current examples as time goes on. We welcome case studies and contributions to this end.

1.2.1 The report structure

This report falls into five parts.

Part 1: a summary report of recommendations and main findings
Part 2: national statutory data collections including a CV at-a-glance age 0-25
Part 3: local data processing including a day-in-the-life of an eleven year old
Part 4: highlights from the transition from compulsory school to Higher Education
Part 5: an annex of data, source materials, research and references.

This is Part 1 and consists of this introduction and summary report to highlight our ten areas of recommended actions. Parts 2-5 are online only.

Part 2 starts by identifying the core infrastructure behind national statutory data collections in the state education system affecting children typically from birth to age 25. We mapped the most common statutory data collections for the purposes of the national accountability system that are about recording a child's attainment and testing and the seven types of census collected by the Department for Education on a termly or annual basis. A subset applies to every child in mainstream education with additional collections for each child who attends state-funded Early Years settings, is a child at risk, or leaves mainstream education and is counted in Alternative Provision. We added in the most common data collections from local level progress and attainment testing for schools' own purposes and additional testing applied to a sample of children nationally every year for national and international purposes. And we address where all this data goes when it leaves a school and how it is used.

Finally we look at samples of other significant pupil data collected through schools about children nationally, such as health data and the vital role of the school vaccination programme as well as the interactions with school settings by other national institutions for youth work, careers or school regulation by Ofsted.

In Part 3 we address local data processing. We map common aspects of the local data landscape and address the data processing from the daily systems and edTech interactions that affect children from both primary, secondary and further education to help readers' understand the volume of data flows between different people and other organisations outside the state education sector. We include a range of case studies picking out different types of edTech most common in schools today.

In Part 4, we address in brief, the transition between school and Higher Education, from childhood to adulthood. We look at some of the most common data processing from applicants and students as they transfer from state education to Higher Education at age 18. We cover both national data collections and local institutional choices processing data for student data analytics and national policies such as the Prevent programme.

Part 5 contains an Annex of tables, and figures including comparisons of national data collections and use across the four devolved nations only to serve as a comparison to England's policy and practice, and while many of the same questions around edTech apply across all of the UK, we do not attempt to map the landscape outside England.

A future and further stage of this project would look to map the Department for Education funding flows across the sector to see where there are differences between who provides data about a child, where the child learns, and who gets the money for providing their education. In researching the Alternative Provision sector in particular the discrepancies indicate a lack of accountability when where a child goes and where the money goes are to different places.

Later guidance will be created from this to help advise teachers and parents of what they can do to protect children's human rights as we continue to move into an ever-more machine-led world.

1.3 Recommendations and selected findings

Three futures need to be championed and must be made compatible in a long term vision for a rights' respecting environment in state education. 1) The rights of every child to education and promotion of their fullest development and human flourishing[19], 2) the purpose and value of learning and education for society and its delivery, and 3) the edTech sector's aspirations and its place in the UK economy and in export. We must build the legal and practical mechanisms to realise rights across the child's lifetime and beyond the school gate, if the UK government is to promote all three. It is against this background that we have undertaken this report at defenddigitalme and recommend founding that framework in legislation upon which that vision for the future can flourish.

1.3.1.1 Recommendations One I Legislation and statutory duties

For national governments

1. Legislate for a UK Education and Digital Rights Act to safeguard the infrastructure behind the delivery of state education and our future sovereign ability to afford, control, and shape it.

2. An Education and Digital Rights Act, with due regard for devolved issues, would build a rights' respecting digital environment in education and consider standards for procurement, accessibility and inclusion; address data justice and algorithmic discrimination, and ensure that introductions of products and research projects to the classroom have consistent pedagogical value, ethical oversight, safeguarding, quality and health and safety standards.

3. Core national education infrastructure must be put on the national risk register. Dependence on products such as Google for Education, MS Office 365, and cashless payment systems, 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.

4. Legislation, Codes of Practice, and enforcement need to prioritise the full range of human rights of the child in education. This should be in accordance with Council of Europe Recommendation CM/Rec (2018) of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment.[20] Stakeholders at all levels must also respect the UNCRC Committee on the Rights of the Child General comment No. 16 (2013) on State obligations regarding the impact of the business sector.[21]

5. An Education and Digital Rights Act would govern not only children's rights to control the access to educational information and records by commercial companies about themselves, but govern rules on routine foreign data transfers and address the implications for the export control, value and security of national public sector created data about our education system through our children's learning and behavioural data held by private companies, in the event of mergers and acquisitions.

[19] 5Rights Foundation https://5rightsfoundation.com/our-work/childrens-rights/ The UN Convention of the Rights of the Child (UNCRC) was first introduced 30 years ago, setting out the conditions in which a child might flourish

[20] Recommendation CM/Rec (2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment https://edoc.coe.int/en/children-and-the-internet/7921-guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-the-digital-environment-recommendation-cmrec20187-of-the-committee-of-ministers.html

[21] Committee on the Rights of the Child General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf

6. Accessibility and Internet access is an economic and a social justice issue. As 1 in 4 children lives in poverty[22], this must come before you promote products on top of the delivery systems. Government should extend the requirement on affordable telephony to broadband to help ensure every child has equitable access to the Internet at home and to keep pace with the connected digital economy to support children in-and-beyond the pandemic crisis response.

7. Ensure a substantial improvement in the support available to public and school library networks. Recognise that children can rely on public libraries for quiet and private study space, particularly those from disadvantaged backgrounds, notwithstanding current COVID-19 limitations.

8. Ensure consistency across the devolved nations for children's biometric data protection. A range of biometric data are processed by commercial companies but the Protection of Freedoms Act 2012 applies only to schools in England and Wales. Introduce legislation on protections of biometric data in Northern Ireland and Scotland consistent with England and Wales, to protect and fulfil the rights of the child in the digital environment across the public sector.

9. Public sector bodies must facilitate mechanisms to explain the Right to Object that accompanies the legal basis under which they carry out most educational data processing under the GDPR Article 6(1)(e) and give families and children a way to exercise it.

10. Freedom of Information laws should be applied to all non-state actors, companies and arms-length government bodies, as pertains to their educational and children's services activities commissioned by the publicly funded state sector.

11. Under s66 of the Digital Economy Act it is a criminal offence to disclose any personal information [obtained] from administrative data for research purposes. Such activity would already be an offence under s.55 Data Protection Act 1998 if undertaken without the data controller's consent. (Mourby at al. 2018)[23] This should be applied to third party commercial data processors that are repurposing administrative data obtained from public sector data processing at local level (a child's pupil data) and disclosing it to third-party researchers that the school did not engage or request that children's data be repurposed.

12. A White Paper should start the ball rolling, to address the sector-wide changes needed, focussed from a people-first and pedagogy perspective. It needs to explore further the rights' issues raised in the pandemic response such as product design and accessibility, infrastructure access and equality, the lack of social contract between children and their data processors; and staff skills; as well as horizon scanning to identify the necessary secure and sustainable infrastructure and governance models required for a safe, just, and transparent digital environment in education.

For the Department for Education

13. A national oversight body is needed on a statutory footing to oversee data governance in education to address the lack and compliance and accountability found by the ICO in its audit of the Department for Education, and issues in the broad use of edTech. A National Guardian for education and digital rights, would provide a bridge between government, companies, educational settings and families, to provide standards, oversight and accountability. Capacity and capability across the sector would further benefit from a cascading network of knowledge with multi-way communication, along the principles of the NHS Caldicott Guardian model.

[22] Child poverty action group facts and figures show the reality of child poverty in the UK https://cpag.org.uk/child-poverty/child-poverty-facts-and-figures

[23] Mourby, M. et al. (2018) Are pseudonymised data always personal data? Implications of the GDPR for administrative data research in the UK https://doi.org/10.1016/j.clsr.2018.01.002

14. Accessibility standards[24] for all products used in state education should be defined and made compulsory in procurement processes, to ensure fair access for all and reduce digital exclusion.

15. A national model of competent due diligence in procurement should be developed and the infrastructure put in place for schools to call on their expertise in approved products. Procurement processes must require assessment of what is pedagogically sound and what is developmentally appropriate, as part of risk assessment including data protection, privacy and ethical impact. Assessment of risk is not a one-time state, at the start of data collection, but across the data life-cycle.

16. Start with teacher training. The national strategy is all about products, when it should be starting with people. Introduce skills, data protection and pupil privacy into basic teacher training, to support a rights-respecting environment in policy and practice using edTech and broader data processing. This will help to give staff the clarity, consistency and confidence in applying the high standards they need. Ensure ongoing training is available and accessible to all staff for continuous professional development. A focus on people, not products, will deliver fundamental basics needed for better tech understanding and use and provide the human support infrastructure needed to reduce workload and investigative burden in school procurement.

17. Establish fair and independent oversight mechanisms of all national pupil data collected in censuses and standardised testing, so that transparency and trust are consistently maintained across the public sector, and throughout the chain of data processing starting from collection, to the end of its life cycle. Develop data usage reports from the Department for Education for each child, that can be downloaded and distributed by schools annually or on request to show individuals what is held about them by the Department and how it has been used.

18. Fix the inconsistency of approach in current legislation that exists between Local Authority and other academy/free schools et al. on the parental right of access to the child's educational record. Standard reports should also be mandated from school information management systems providers to address the inconsistency of how Subject Access rights are fulfilled by the wide variety of school information management systems. Shift the power balance back to schools and families, where they can better understand what is held about them by whom and why.

19. Every company that has a seat at the national Department for Education UK edTech strategy table, or that can benefit from access to public sector pupil data, should also have statutory obligations to demonstrate full transparency over their own sector practices, including business models, extent of existing market reach, future intentions, and meeting data protection law.

20. The Department for Education's statutory guidance 'Keeping Children Safe in Education'[25] obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place"* but gives no guidance how to respect privacy and communications law or rules on monitoring out of school hours or while at home. This needs urgent regulatory intervention and changes in legislation to prevent today's overreach that affects millions of children at home in lockdown and while remote learning. (See case studies, part three) Defining safeguarding in schools services and software application standards

[24] The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 https://www.legislation.gov.uk/uksi/2018/952/regulation/4/made

[25] The Department for Education's statutory guidance 'Keeping Children Safe in Education source 2018 https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

could begin in the short term as consultation with industry and civil society, and lead to a statutory Code of Practice.

21. To ensure respect for the UPN statutory guidance[26] that states the UPN must lapse when pupils leave state funded schooling, at the age of sixteen or older, the Department for Education should clarify what 'lapse' means in accordance with the law, for retention and data destruction policies.

For Local Authorities and Multi-Academy Trusts and educational settings

22. Public Authorities should have a duty to carry out a Child Rights Impact Assessment before any adoption of large scale or high risk projects involving children's data obtained through schools. Public Authorities should document and publish a transparency and risk register of such projects, and any data distribution, including commercial processors /sub processors terms of service, any commercially obtained sources of personal data collected for processing.

23. Public Authorities should include a duty to document routine large-scale linkage of administrative data processed about individuals in the course of their public sector interactions (Dencik et al 2019) as part of ROPA (GDPR Article 30) and in particular where such data is used for predictive analytics and interventions. Re-use should be made transparent and registers updated on a regular basis. (i.e. Data bought from brokers, third-party companies, scraped from social media) Data Protection Impact Assessments, Retention schedules, Procurement spending on data analytics and algorithm should be published as open data, and GDPR s36(4) Assessments published with regular reviews to address changes to contribute to a improved cumulative national transparency.

24. Public bodies at all levels must respect the Right to Object that accompanies the legal basis under which they carry out most data processing under the GDPR Article 6(1)(e). Local Authorities and educational settings must enable consistent ways to explain to children and parents when they have a right to object and offer ways to exercise it and processes to make the balancing test and communicate its outcome, where it applies when processing personal data under the public task at all levels.[27] (GDPR Articles 6(1)e, 9, and Recitals 69 and 70). Staff must be trained on their obligations and how to fulfil them.

25. All educational settings must have a statutory entitlement to be able to connect to high-speed broadband services to ensure equality of access and participation in the educational, economic, cultural and social opportunities of the world wide web.

26. Ensure respect for the UPN statutory guidance[28] in retention and data destruction policies that states the UPN must lapse when pupils leave state funded schooling, at the age of sixteen or older.

27. Furthermore, the UPN must be a 'blind number' not an automatic adjunct to a pupil's name. It must be held electronically and only output from the electronic system when required to provide information to:

    - Local authority
    - central government
    - another school to which the pupil is transferring

[26] Unique pupil numbers (UPNs) (2019) A guide for schools and local authorities, version 1.2 https://www.gov.uk/government/publications/unique-pupil-numbers

[27] Information Commissioner (ICO) | The right to object to the use of your data [processing under the public task] https://ico.org.uk/your-data-matters/the-right-to-object-to-the-use-of-your-data/

[28] Unique pupil numbers (UPNs) (2019) A guide for schools and local authorities, version 1.2 https://www.gov.uk/government/publications/unique-pupil-numbers

- a third party (for example, a supplier of a schools management information system) who have entered into an agreement to provide an education service or system to a school, local authority or government department and process data on their behalf
- A pupil's admission number, rather than the UPN, must be used as the general pupil reference number on the admission register or paper files.
- The sharing of UPN data with a third party for work or a service not commissioned by the school, local authority or another prescribed person is not permitted nor would the sharing of UPN data for any purposes not related to education.

1.3.1.2 Findings 1 I Legislation and statutory duties

28. Nesta proposed in its 2019 report, Educ-AI-tion Rebooted?[29] that the Government should publicly declare an ambition to create a system of responsible education data sharing by 2030. That somewhat suggests that they believe we do not have one today. We agree with both positions but suggest that 2030 is too far away and the governance framework must start to be built with urgency.

29. The State delivery of education cannot reliably depend long term on the planning of private providers, or their free-for-first-three-months offers, to deliver critical educational infrastructure on which both the public sector and the ability to go-to-work of millions of parents rely.

30. Rapid response by the Department for Education to support schools without any remote learning platform was exclusively supportive of the 'Big Two' Google and Microsoft, and indirectly supported their market foothold. Yes," *many educational settings lack the infrastructure"* but that should never mean encouraging ownership and delivery by only closed commercial partners. The current route risks the UK losing control of the state education curriculum, staff training and (e)quality, its delivery, risk management, data, and cost controls.

31. At national level there is no independent oversight of how any data infrastructure at local and regional school level is managed. The delivery of education fails to appear on the national risk register despite its brittleness and the problems in its vulnerability caused by remote learning demands in response to the shock of the COVID-19 pandemic. Who owns and has responsibility for the infrastructure? How much is dependent on Silicon Valley and what is known about future ownership, stability, security and costs? Where is it inadequate? Does it meet national needs from the child's educational perspective? What plans exist if a company that provides its products plus teacher training for free today, nationwide, starts charging tomorrow?

32. It is not within OSR's current remit to regulate the operational use of algorithmic models by the government and other public bodies. Where this regulation should sit needs to be decided and put on a statutory footing after the review of the 2020 exams awarding process.

33. Questions of accountability, funding and data are inextricably linked, but when it comes to managing the digital child, there is often confusion over who is responsible for what information when. And the sensitivity of digitized pupil and student data should not be underestimated.[30]

34. To guard against Department for Education reputational risk and if the national edTech sector is to be successful in its home grown support of children's learning and administration as well

[29] AI Educ-AI-tion rebooted? Exploring the future of artificial intelligence in schools and colleges (2019) Nesta | https://www.nesta.org.uk/report/education-rebooted/

[30] International Working Group on Data Protection in Telecommunications (2017) Working Paper on e-learning platforms https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2017/2017-IWGDPT_Working_Paper_E-Learning_Platforms-en.pdf

as in an export strategy, national and local level changes are needed to ensure product integrity and safety standards are achieved.

35. Data protection law fails to take account of emerging technologies that process information about children's bodies and behaviour but that do not meet the definition of biometric data. Data protection law alone cannot offer children adequate protections when it comes to product trials and research trials or controls, involving children without parental consent.

36. Data protection law is insufficient to protect children's full range of rights in the digital environment. Only by reshaping the whole process for the long term, will we have a chance to restore the power balance to schools and to families. Schools must return to a strong position of data controllers and delegate companies to data processors with consistent standards on what they are permitted to do. That infrastructure may not exist, but we need to build it.

37. Start with designing for fairness in public sector systems. Minimum acceptable ethical standards could be framed around for example, accessibility, design, and restrictions on commercial exploitation and in-product advertising. This needs to be in place first, before fitting products 'on top' of an existing unfair, and imbalanced system to avoid embedding disadvantage and the commodification of children in education, even further.

38. While the government is driving an edTech strategy for post-Brexit export, it fails to adequately address fundamental principles of due diligence. This needs to go beyond questions of data protection which is a weak protection for children, disempowered in the domestic public sector environment. A child rights framework is needed to ensure high standards generate the safe use of UK digital products worldwide, not only in the school life of a child, but for their lifetime.

39. Finding a lawful basis for children's personal data processing for many emerging technologies is a challenge. For example, many apps' and in particular AI companies' terms and conditions may set out that they process on the basis of consent. But children cannot freely consent to the use of such services due to capacity and in particular where the power imbalance is such that it cannot be refused, or easily withdrawn. *"Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent."* (ICO)

40. Consent and contract terms must be rethought in the context of education and for children and their legal autonomy at age 18 and clarified with schools. As set out by the European Data Protection Board in 2020 Guidelines on consent[31], children [and their guardians] cannot freely consent to data processing, where the nature of the institutional-personal power imbalance means that consent cannot be refused, or easily withdrawn without detriment, and they recognise that the GDPR does not specify ways to gather the parent's consent or to establish that someone is entitled to perform this action or how consent should expire from parents and be asked of a young adult.

41. There are also problems with understanding the shared roles of child/parental consent that data protection law fails to address for educational settings where processing is primarily part of a public task. Collecting flawed consent is routinely used as a tick box exercise, and not the proper communications process that it should be to explain what tool is used, how and why.

42. At the local level the proliferation of apps used in educational settings for administrative purposes, or to support learning and special needs or wellness interventions has no oversight. Although many digital tools market themselves as meeting Ofsted standards or to help schools do well in inspections, the Inspectorate plays no role in the standards of digital rights

[31] European Data Protection Board Guidelines 05/2020 on consent under Regulation 2016/679
https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

or safety and these marketing claims may be baseless when the regulator has not approved them.

43. One academy Trust cites over 85 third-party companies and organisations in a non-exhaustive list that interact with children's daily lives, some of whom will in effect also have access to 'peer into parents' phones' too, when they use the parent app to view children's school records, update the cashless payment system, notify school of absence or view the behaviour-points their child earned that day.[32]

44. While schools must only hire staff to work with children after DBS checks and due diligence, anyone can set up a technology company without financial background or safety checks and get into children's lives and seek to influence them online without any independent oversight. Some edTech can be very intrusive but in ways that may not be apparent to parents. Some products can take photos via a child's webcam. Some digital tools enable companies to find out about children's mental health and identify the most vulnerable; and the companies then seek to engage in life-long relationships with millions of children who were required to use the product simply because they went to a school that chose to let them into the children's lives.

45. With no minimum pedagogical or safety standards, hundreds of apps and platforms can influence which books a child will read, shape if they like a subject or not, determine what behaviours are profiled. They can advertise straight to parents' mobile phones to influence their personal choices or pitch upgrades from the free product the school chose to use, to the premium product that parents pay for. While some tools offer parental portals they often focus on presenting their own perceived added value: dashboards, monitoring reports and even giving parents copies of children's every move, an itemised list of food and drink bought in the canteen, or behaviour recorded in school systems.

46. None offers sufficient insight into how the company behaves or shows how the child's data they process is shared with affiliated companies, sets out what advertisers parents should expect to see on their mobile phones, or how algorithms use a child' data to monitor or predict their behaviours and influence a child's educational experience.

47. The constant commercial surveillance of our online behaviours that the adTech online advertising industry is built on; knowing when you use a product, for how long, where you click, which pages you stay on and where you go next online when you leave an app; is deeply embedded in much of the edTech industry. As set out in the UNICEF issue brief no.3 in August 2020 on good governance of children's data, government policies in countries around the world offer only limited protections for young people in this expanding, commercialized media culture. (Montgomery et al. 2020)

48. The values and educational vision that sit inside products are hidden in black-box algorithms embedded in a child's daily school life in the classroom and beyond, as a result of school-led procurement. Algorithms with hidden biases and unintended consequences are used in educational settings from low-level decisions, such as assigning class seating plans based on children's behavioural scores to shaping their progress profiles every day. AI might be shaping an adaptive curriculum or assigning serious risk classifications about Internet activity.

49. Internet monitoring that operates whenever a child, teacher or school visitor connects to the school network or GSuite environment, can surveil screen content and searches, by analysing everything the user types or receives on their device, even passwords[33] including on personal devices depending on the school policy and provider of choice. Some systems can capture text every thirty seconds until the user has stopped or performed an action. If the device is

[32] Who do we share data with? John Taylor Multi Academy Trust (January 2020) https://jtmat.co.uk/privacy/who-do-we-share-data-with/ archived https://web.archive.org/web/20200911170527/https://jtmat.co.uk/privacy/who-do-we-share-data-with/

[33] Smoothwall Frequently Asked Questions https://kb.smoothwall.com/hc/en-us/articles/360002135724-Frequently-Asked-Questions-FAQs-

offline, text capture might be sent as soon as it reconnects. Some use AI to match what is typed on-screen with thousands of keywords, which can even include items a child subsequently deletes, suggesting that a child is a risk to themselves or to others, or at risk from radicalisation and label a child's online activity with 'terrorism'. Many of the monitoring may continue to work out of school, offsite and out of hours as long as the connection to the school network or GSuite environment remains. Most families we polled in 2018 do not know this. Or know that their child's on- and offline activity may continue to be surveilled remotely through school software, devices or services during lockdown, or routinely at weekends and in the summer holidays.

50. The UNCRC Committee on the Rights of the Child General comment No. 16 (2013) on State obligations regarding the impact of the business sector require that:

> *"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."*

51. The use of biometrics is not routinely permitted for children in other countries as it is in the UK.

52. Putting high standards and oversight of these sensitive processes in place would not only be good for learners. Schools need clarity and consistency, to have confidence in using technology and data in decisions. Companies big and small, need a fair, safe, and trusted environment if a sustainable edTech market is to thrive.

53. An alternative model of data rights' management in education works in the U.S., governed by FERPA with local state variations. It offers a regional model of law and technical expertise for schools to rely on, with standard trusted contractual agreements agreed at the start of a school year on a regional (State) basis with technical expertise appropriate to the necessary level of due diligence edTech can demand.

- Schools are data controllers. Processors cannot change terms and conditions midway through the year, without agreed notification periods, and reasonable terms of change.
- Families get a list each year (or at each school move) to explain the products their child will be using and legal guardians retain a right to object to products.
- Schools are obliged to offer an equal level of provision via an alternative method of education, so that objection to the use of a maths quiz app is not to the detriment of the child and they do not miss out on teaching.

"*In the U.S. Between 2013 and 2018, 40 states passed 125 laws that relate to student privacy. In general, these have coincided with states moving to online statewide testing (which has increased the quantity of data created and shared) and as states have built integrated data systems that combine data from multiple state agencies. Some common goals of these laws are*

- *building upon FERPA and PPRA by further restricting what student data a school can collect or share with others*
- *providing further requirements and guardrails related to student data shared with websites, online services, and applications*
- *designating a chief privacy officer and other individuals at the local level responsible for ensuring compliance with privacy laws*
- *requiring more transparency about what data schools collect and what it is used for*

- *requiring that schools and vendors meet certain data security standards*
- *requiring notification to parents in the event of a data security breach."* (Student Privacy Compass, 2020)[34]

54. There is a public demand for greater accountability from technology companies. Two thirds asked in the DotEveryone survey for the People, Power and Technology the 2018 digital attitudes report[35] said "*the government should be helping ensure companies treat their customers, staff and society fairly. People love the internet—but not at any cost. When asked to make choices between innovation and changes to their communities and public services, people found those trade-offs unacceptable."*

55. The Library and Information Association has pointed to the Chartered Institute of Public Finance and Accountancy figures of a net reduction of 178 libraries in England between 2009-10 and 2014-15.[36]

56. Educational settings rarely respect the Right to Object that may apply when processing personal data under the public task 'in the exercise of official authority'. This covers public functions and powers that are set out in law; and there are no mechanisms for schools to communicate when and why the right applies, the process, or for children and families to exercise this right in national statutory data collections or the collection of local administrative data or in digital tools that process data for marketing. (GDPR Articles 6(1)e, 9, and Recitals 69 and 70)

57. Due to inconsistent legislation, parental access rights to your own child's school records is not standardised for children across all settings as regards rights to the educational record and inconsistent between Local Authority and academies and other models of education.[37]

58. Standard reports to meet data protection law vary wildly between school information management systems providers and generate inconsistency in how Subject Access Rights are fulfilled by a wide variety of settings. Schools can struggle to meet SARs due to the way in which information is managed, and some offer limited system ability to generate legally required documents. In a quid pro quo for MIS providers to access the public sector they should be required to demonstrate a high minimum standard requirement to support schools' needs.

1.3.2.1 Recommendations Two I Assessment, Attainment, Accountability, and Profiling

While many may consider the middle of a pandemic not the best time to restructure school assessment, progress, and accountability measures, it is inevitable since some of the mainstays of the system do not exist for some year groups after their cancellation under COVID-19. The Department for Education Data Management Review Group 2016 findings are yet to be realised, so that schools can have greater freedom to balance professional autonomy and agency against the demands of the accountability system. And the recommendation from the 2017 Primary Assessment enquiry has not been realised to ensure the risks "of schools purchasing low-quality assessment systems from commercial providers" are mitigated against through standards' obligations. This year's awarding process and its failure of fitness for purpose also demonstrates a need for better

[34] Student Privacy Compass (2020) https://studentprivacycompass.org/state-laws/

[35] Miller, C., Coldicutt, R. and Kos, A. (2018) DotEveryone Attitudes Report http://attitudes.doteveryone.org.uk/

[36] Nearly 130 public libraries closed across Britain in the last year (2017-8) and disproportionately affects children Research Library Briefing paper Number 5875, 20 June 2019 https://www.theguardian.com/books/2018/dec/07/nearly-130-public-libraries-closed-across-britain-in-the-last-year https://defenddigitalme.com/wp-content/uploads/2019/11/SN05875.pdf

[37] The Education (Pupil Information) (England) Regulations 2005 do not apply to non-maintained schools (e.g. academies, free schools and independent schools). https://www.legislation.gov.uk/uksi/2005/1437/contents/made

risk assessment and understanding of the potential for discrimination in data, across all of these systems at all levels.

For the Department for Education

59. Urgent independent statistical assessment must be made of the modelling using Key Stage 2 and GCSE prediction reference grades for the 2021 GCSE exam awards process, and the A-levels grading system, including assessment for bias and discrimination in data and design. Obligations on algorithmic explainability need met in ways that meet student needs in plain English and we propose an individual level report that educational settings (exam centres) can download that will demonstrate any data sources, calculations and how each grade was awarded at individual level. The Office for Statistics Regulation (OSR) Review may wish to address this.

60. The Department for Education should place a moratorium on the school accountability system and league tables 2020-25 while an assessment is carried out on fitness for purpose.[38] Recognising where pupil data will continue to be affected by COVID-19 making comparable outcomes and competitive measures meaningless and progress measures may be misleading, this means a pause on EYFS, Baseline, MTC, KS1, and only sampling Phonics and a sample population could sit the KS2 SATs or alternative assessment where preferable.

61. Support 2021+ Primary into Secondary school transition beyond the national sampling of KS2 SATs scores, with KS2 SATs or similar year 6 assessment used for local area use only, in context, and for school transfers, building a fair and lawful decentralised data model, based on the six-into-seven principles, allowing staff to concentrate on children's local needs.[39]

62. Carry out an independent national review and a Child Rights Impact Assessment of the state school accountability, local and national progress measures, and benchmarking models— including those designed by commercial providers and sold to the public sector— to assess for lawfulness and safeguards to prevent harm from individual profiling (aligned with the GDPR Article 25 and recital 71) since such measures 'should not concern a child'.

63. The Department for Education should correct its national guidance,[40] *"There Is no need for schools to share individual Progress 8 scores with their pupils"*. This instruction from the Department for Education leads to unfair data processing practice by schools in breach of the first data protection principle.

64. The Reception Baseline Assessment should not go ahead. It must be independently re-assessed for compliance with data protection law and algorithmic discrimination in a) its adaptive testing model design b) Right to Object c) the plans for seven-year score retention and d) decision to not release data to families. The pilot and trial data were not collected with adequate fair processing.

65. Who watches the watchdog? All reuse of historic datasets for regulatory oversight by Ofsted should be independently assessed for discrimination as identified in the 2020 exams awarding process. While it is not within OSR's current remit to regulate the operational use of models by the government and other public bodies where this regulation should sit needs to be decided and put on a statutory footing.

66. Every expansion of the seven school censuses and standardised testing should require public consultation and affirmative procedure before legislation can expand national data collections.

[38] Goldstein, H. and Leckie, G. (2008) School league tables: what can they really tell us? https://doi.org/10.1111/j.1740-9713.2008.00289.x Significance. Vol.5 Pages 67-69

[39] Supporting Primary to Secondary school transition https://opendataproject.org.uk/sixintoseven/

[40] Progress 8 national guidance issued by DfE page 3 http://defenddigitalme.com/wp-content/uploads/2018/04/Progress_8_and_Attainment_8_how_measures_are_calculated.pdf

67. The recommendation from the 2017 Primary Assessment enquiry has not been realised to ensure the risks "of schools purchasing low-quality assessment systems from commercial providers" are mitigated against through standards obligations.

68. Teacher training in statistics and understanding bias and discrimination in data is required to inadvertently perpetuate any historical bias in schools data that staff have to interpret, including socio-economic, ethnic, and racial discrimination.

69. Right to explanation and fair processing must become routine and realised across all school settings. Attainment test results and progress measures must be made available to pupils and families and cannot be carried out in secret or the results black-boxed (aligned with the GDPR Articles 12-15, 22(2)(b) and 22(3)). A standard process must be designed to enable this two-way communication and offer meaningful routes to address questions and seek redress.

70. Privacy and Data Protection Impact Assessments should be routinely carried out and published before any new national test, new data collection or new processing aim is announced, especially where it concerns profiling, sensitive data types or the use for punitive purposes. The assessment should be independent from organisations involved as data users and be published. (aligned with the GDPR Article 22(2)(b)).

1.3.2.2 Findings 2 I Assessment, Attainment Profiling and Accountability

71. The summer 2020 exams awarding process was always going to be hard. But then it resulted in the Prime Minister making claims about mutant algorithms and the resignation of the Chief Regulator of Ofqual. Its risk assessment[41] was signed off only a day before the publication of GCSE results which appears odd given it is after any data processing was carried out.

72. There were no Key Stage 2 SATS tests and yet primary age children have successfully transitioned from year six into seven. There was no accountability data sent to the Department for Education and although there are no progress 8 measures calculated for this year's cohort, teaching and learning continues.

73. The pause on standardised testing in 2020 shows that it is possible. Leckie and 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 they have often been to date.*[42] With respect for the late Harvey Goldstein perhaps it is the right time like no other, for the government to recognise his 2008 assessment of school league tables. They are not fit for purpose.[43]

74. Progress 8 was intended to measure the impact a secondary school has on a pupils' performance across eight subjects. It uses the Key Stage Two results of pupils in their last year at primary school as a starting point. It is a flawed and unsuitable measure of individual *ability* at age 10 designed as it is to measure *system accountability*, and almost certainly of dubious value to repurpose for reference in GCSE grade modelling, through its reinforcement of feedback loops.

[41] The Ofqual Data Protection Impact Assessment (summer 2020) https://defenddigitalme.org/wp-content/uploads/2020/09/Data-protection-impact-assessment-summer-2020-grading-1.pdf

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

[43] Goldstein, H. and Leckie, G. (2008) School league tables: what can they really tell us? https://doi.org/10.1111/j.1740-9713.2008.00289.x Significance in 2011). Vol.5 Pages 67-69

75. Gaming the system by primary schools or parents, can affect the results for those pupils and therefore the accountability measure as a “value-add” of the secondary school. Pupils may not go on to measure up to their expected attainment level, between age 10-11 and GCSEs taken at age 16. Judging secondaries by Progress 8 is therefore a mechanistic but rather meaningless measure, and it is commonly accepted that some primaries data is inflated through above average test preparation by the school or parents beyond what may be expected.

76. All pupils with KS1 results are slotted into PAGs alongside thousands of other pupils nationally. The DfE then takes in all the KS2 test scores and calculates the average KS2 score for each PAG. The result is a made-up metric distorted by the pressures of high stakes of accountability. (Pembroke, 2020b)

77. Without teacher training in statistics and understanding bias and data discrimination, teaching staff are likely to inadvertently perpetuate any historical bias in the data they have to interpret. Given the significance of carrying out assessment it is a big gap in teacher training, as Dr Becky Allen told the Education Select Committee Enquiry on primary assessment in 2017, that “we do not have a system of training for teachers that makes them in any way experts in assessment”. Some schools had resorted to buying commercial options of varying quality, as described by the Association of Teachers and Lecturers concerned about several dubious “solutions” commercially available to schools which do not offer value for money or a high-quality assessment framework. It was proposed in 2017 that the risks “of schools purchasing low-quality assessment systems from commercial providers” are to be mitigated by high quality advice and guidance, rather than change of policy and practice. That recommendation from the enquiry into Primary Assessment has not been realised and must be with strengthened standards requirements.

78. Children and parents have the right to obtain human intervention in any automated decision making, to express his or her point of view and to contest the decision. Accountability measures that routinely profile a child fail to address these rights today, and furthermore require change to build human safeguards into the process so that any errors are easy to identify, the outcomes easily understood by the staff and parents, and any effects as a result explained to both. Fair processing is required to explain what data has been collected and how it will be processed.

79. Individuals have rights to access data, and request correction of inaccurate personal data. A person has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on either the GDPR Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

80. The Department for Education Data protection: toolkit for schools (2018)[44] fails to inform schools to apply this right to all statutory high stakes testing and school census data collections, how to do so, or provide any mechanism for families to make an objection to the Department for Education as the data controller.

81. This applies to all data processing across the collections in the accountability system and must be applied in the case of the Reception Baseline Assessment as well as to all other statutory high stakes tests and school census data collections.

[44] DfE Data protection: toolkit for schools (2018) https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

82. The Reception Baseline Assessment has a number of significant problems with the test approach as regards data protection law and in its design. It is problematic from an equality and disability rights perspective given that the same approach is not inclusive for all. When we reviewed the Data Protection Impact Assessment for the Baseline Test,[45] we found it omitted many of the risks including its adaptive test design, omitted that reasons for not taking the test were collected, and did not mention how data may be accessed by third parties from the National Pupil Database. We have been unable to get an answer from the NFER or Department as at September 2020, how they believe it meets the full range of legal obligations of UK data protection law. We were told by an NFER spokesperson in September 2020, that the Department is currently reviewing the DPIA and the privacy notices in advance of the assessment becoming statutory (in 2021). Given the DfE release of data to third parties (including policing, DWP fraud investigation and for the purposes of the Hostile Environment) our opinion is that the rights of individuals to protections of rights and freedoms outweigh those of the Department, and distribution goes further than fair processing and parents' reasonable expectations. The Reception Baseline Assessment, for national purposes, should not proceed.

83. The Department for Education Data Management Review Group 2016 report with the aim of reducing teacher workload had a finding we can strongly support four years later. *"Government, school leaders, and teachers, rather than starting with what is possible in collecting data, should challenge themselves on what data will be useful and for what purpose, and then collect the minimum amount of data required to help them evaluate how they are doing. Decisions about the identification, collection and management of data should be grounded in educational principles. In this way schools can have greater freedom to balance professional autonomy and agency against the demands of the accountability system."*[46]

84. By contrast no work has been carried out from a child's perspective or considering legal obligations towards data protection and privacy seen through the lens of children's rights for the extensive research trials and innovation fund interventions. This should be done urgently through child rights' impact assessment.

85. The Core Content Framework for Initial Teacher Training[47] in England, which sets the parameters for a minimum entitlement in initial teacher education makes no reference to technology-supported learning, or digital rights, or data literacy skills despite the vast amount of assessment and accountability measures. This must change and become part of basic teacher training.

[45] The Data Protection Impact Assessment for the Baseline Test (RBA) https://www.whatdotheyknow.com/request/baseline_data_protection_impact

[46] Department for Education Data Management Review Group (2016) Reducing teacher workload: Data Management Review Group report https://www.gov.uk/government/publications/reducing-teacher-workload-data-management-review-group-report

[47] Core Content Framework ITT (2019) https://www.gov.uk/government/publications/initial-teacher-training-itt-core-content-framework

Fig.1 overleaf is an infographic to demonstrate the range of sources of data that may become part of a child's national pupil database record in England, over the course of their lifetime education age 5-19. The records for a child that attends state funded Early Years educational settings will start earlier, any time from the rising 2s. A child at risk, may be captured in data from before birth if they are the child of a child, whose personal records will be sent to the Department for Education in the Children in Need (CIN) Census. Not every child will experience Alternative Provision or transition to Higher Education. But those who do, will have a larger named pupil record at national level. Personal data is sent to the Department for Education from every statutory test a child takes from the Early Years Foundation Stage Profile, to Phonics Tests, SATs and GCSE and A-Levels and more. The core data about a child are extracted in nearly every termly school census, annual census, and statutory test. Where this deviates is noted. Some items have multiple sub-categories of detail but we do not list them all in the chart, including SEND types that may be Autism Spectrum Condition (ASC), Speech, Language and Communication Needs (SLCN), Specific Learning Difficulties (SLD), Moderate Learning Difficulties (MLD), Social, Emotional and Mental Health Difficulties (SEMH), Attention Deficit and Hyperactivity Disorder (ADHD) and Sensory and/or Physical Difficulties.

Data from the National Pupil Database* are distributed to a wide range of third parties. We believe it is unnecessary and disproportionate for many of these details to be retained by the Department for Education indefinitely at named pupil level, and instead data could be extracted in anonymised, aggregated groups of data, or through statistical sampling.

If you want to help us change this, please write to your MP and tell friends and family. You can see more information and steps to ask to see what is held in your own or your child's record (since 1996) at: https://defenddigitalme.org/my-records-my-rights/

NB. *Selected CIN data are not added to the NPD and some are restricted to Department for Education staff only.[48]

[48] *FOI request: Pupil data: Children-in-Need Census expansion (WhatDoTheyKnow) https://www.whatdotheyknow.com/request/pupil_data_children_in_need_cens#incoming-1639044

Fig 1 A National Pupil Database record over a child's lifetime

My National Pupil Database Record

About a Child

This personal data is collected in each statutory assessment and census collection unless otherwise indicated

First name
Last name
Middle name(s)
Former names
Date of Birth
Gender
Ethnicity
First language
Special Educational Needs and Disability
Home address*
Unique Pupil Number (UPN) 0+
Unique Learner Number (ULN) 14+
Any former UPN

*If a child has multiple addresses (i.e. if a child lives with both parents at different stages of the week) both are included in the school census, plus location data codes, UKPRN

Any archived items:
Nationality (2016-18)
Country of birth (2016-18)
Statemented

All this personal data is also core to each census plus personal indicators and school assigned characteristics, to which the further items of each census are added

Statutory national assessment data collections

Pre-school (Age 2-4) Early Years Foundation Stage Profile

UPN	Home postcode
Full names	Local Authority Number (LAN)
Date of birth	Establishment (school number)
Gender	Subject, component and result (1, 2, 3 or 4)

Reception (Age 4-5) Reception Baseline Assessment

Personal data plus the raw scores from the assessment out of 25 as well as reasons for not taking the test

Year 1 (Age 5) Phonics Screening Check

Personal data and Establishment characteristics (school details incl. religious character and funding) plus the total score from the phonics test. Outcomes summary, meeting or not meeting the expected standard. Curriculum year group and raw mark are required as well as reasons why child did not take the test. Schools can continue to assess pupils using P scales 1-4 for children not meeting the expected standard in 2020/21

Year 2 (Age 6-7) Key Stage One SATs

Personal data and Establishment characteristics as in previous assessments plus assessment with scaled scores from Key Stage One SATs Maths (Arithmetics and Reasoning), Reading, Writing and (optional) Spellings, punctuation and grammar test (SPaG)

Year 4 (Age 8-9) Multiplication Times Table Test

Personal data and Establishment characteristics as in previous assessments plus the scores for Multiplication Times Tables Test and any reasons for not taking the test; including English as an additional language

Year 6 (Age 10-11) Key Stage Two SATs

Personal data and Establishment characteristics as in previous assessments plus assessment with scaled scores from Key Stage One SATs Maths, Reading, SPaG, and (optional) Science

Years 10-11 (Age 15-16) GCSE and other qualifications (KS4)

Exam results and further personal data from GCSE and iGCSE, BTEC, technical and vocational qualifications

Years 12-13 (Age 17-18) A-Level and other qualifications (KS5)

Exam results and further personal data from A-levels, A-S levels, IB, vocational or technical qualifications (VTQs) and T-level placements

Statutory national census data collections

- **Early Years Census (Annual age 2-5)**
- **School Census (Termly age 2-18)**
- **PLAMS Post-16 Learning Aims (Termly 16+)**
- **Higher Education Statistics Authority data (on entry)**
- **Alternative Provision Census (Annual age 2-18)**
- **Looked After Children Census (Annual age pre-birth - 21)**
- **Children in Need Census (Annual age pre-birth - 25)**

Early Years Census

About a Child
plus
Early Years pupil premium
2-year-old basis for funding and 30-hour code
Class information (nursery class or not)
Funded universal entitlement
Hours at setting and unit contact time
Ofsted EY unique reference number
School childcare
Setting address, hours, staffing and contact details

School Census

About a Child
Personal Indicators
School-assigned Characteristics
plus
Admission appeals
Enrollment status
Exclusions for both on and off roll pupils
Home information
Learning support code
Post looked-after arrangements
PRU or AP provision indicators
Pupil data of entry
Pupil date of leaving
School identifiers and Establishment number
Termly attendance*
Various funding details

PLAMs Census

Year 12 and above have additional data collected once a year in the autumn School Census about learning aims, traineeship, and Maths and English GCSE prior attainment

Personal Indicators on a Pupil Record

Adopted from care
Disability access fund indicator (3-4 year olds)
Family in the armed services
Free school meals (pupil premium eligible)
FSM eligibility start date
In care
Member of SEN unit
Post looked after arrangements
Pupil medical flag
Pupil part-time or boarder
SEND type and ranking
Youth Support Services agreement

School-assigned Characteristics

Attendance data
Local Authority number
National curriculum year group
School identifiers and establishment number
School lunch taken
Type of school and funding details

Alternative Provision Census

About a Child
Personal indicators on each pupil record
School-assigned characteristics
plus
Attendance pattern
Exclusion and reasons for exclusion(s)
Home information
Placement module
Reasons for transfer
SEN provision
URN previous school

Looked After Children Census

About a Child
Personal Indicators
plus
Date of birth of mother's child
Details on adoption or guardianship
Episode of care information
Immunisations/ Dental /Health data
Missing children data
Motherhood status (is the child a mother?)
Placement details
Substance misuse
Unaccompanied asylum seeking children status

Children in Need Census

Categories of abuse**
Child protection conference and plan start date
Data on other household members
Date of birth
Date of death
Disabilities (12 categories)
Ethnicity
Expected date of birth (referrals of unborn children)
Gender
Local Authority child ID
Section 47 enquiry details
Source of referral and date
Unique Pupil Number (UPN) can be assigned pre-birth

Higher Education Equality Monitoring

This optional monitoring data, if collected, is at named individual level in UCAS applications and passed on by HESA to the Department for Education which adds them to the named record in the National Pupil Database

Religion | Sexual orientation | Gender reassignment
Sex | Disability | Ethnicity | Marriage/Civil partnership
Caring responsibilities | Pregnancy and maternity

In 2020-2021* the DfE intends new Regulations to collect all attendance data rather than just those that equate to authorised and unauthorised absence and the CIN census** categories of abuse data will be further expanded

1.3.3.1 Recommendations Three I Admin data collections and national datasets

The ICO summary of its compulsory audit of the Department for Education data handling is damning.[49] Lack of oversight, accountability and lawfulness. National data collections of highly sensitive data have been rushed through successive parliaments in negative secondary legislation that far outstrip the data collection intentions of the original Education Act 1996 or squeezed into surprising places in non-education based legislation. Changes are needed in the making of legislation, risk assessment, re-use and repurposing of national pupil datasets, research access, and recognition of rights. Some national practice is currently unlawful, unsafe, and unaccountable. This needs substantial work to be fit and proper foundation on which to build a national data strategy[50] "to drive the collective vision that will support the UK to build a world-leading data economy." To be of greater value to users and reduce tangible and intangible costs to the state at national, local authority and school levels, national datasets should be reduced in size and increased in accuracy. The current direction of travel is ever more data and 'mutant' algorithms, when it should be towards more accurate and usable data within a trusted regime with standards, quality assurance and accountability. This needs action if the national data strategy is to become more than an aspiration.

For Government at national level

86. The Government should set out a roadmap towards a system of responsible education data including a governance framework and independent oversight by 2030, in a white paper for an Education and Digital Rights Act. Interim steps should be sooner.

87. The government sets out its aim in the Digital Charter[51] to give people more control over their personal data through the Data Protection Act, and to protect children and vulnerable adults online. We suggest that this should start in education by recognising the need for change of its own practices at national level to protect children's confidential personal data from use by third parties and for purposes far beyond our reasonable expectations.

88. The Secretary of State for Education must act on the recommendation from the 2014 Science and Technology Committee Report, Responsible Use of Data; "*the Government has a clear responsibility to explain to the public how personal data is being used.*[52]

For the Department for Education

89. The Department must address all of the ICO findings in a timely manner and publish its changes to restore public and professional confidence in its data handling capabilities.

90. Independent oversight should be established on a statutory footing for education data as a national data guardian responsible for national children's data, and supporting educational settings with expertise in research ethics, algorithmic accountability and public engagement.

91. Following its ICO audit and the national Learning Records Service breach[53] an independent audit should be carried out of the reuse of children's personal confidential data from all national pupil datasets, distributed to third-parties, at national level.

[49] ICO (2020) Statement on the outcome of the ICO's compulsory audit of the Department for Education https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/statement-on-the-outcome-of-the-ico-s-compulsory-audit-of-the-department-for-education/

[50] The UK National Data strategy (updated September 2020) https://www.gov.uk/guidance/national-data-strategy

[51] The Digital Charter (2019) Policy paper https://www.gov.uk/government/publications/digital-charter/digital-charter#approach

[52] Science and Technology Committee Report 2014-15 http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf

[53] Trandall, S. (2020) Civil Service World | DfE data protection 'tightened significantly' after massive breach of learner records https://www.civilserviceworld.com/news/article/dfe-data-protection-tightened-significantly-after-massive-breach-of-learner-records

92. Introduce, improve and publish routine audit reports of third-party data distribution. The Department must be able to audit which child's information was used in which third-party release and proactively provide this information as part of national Subject Access Requests.

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

94. The Department for Education must ensure data minimisation in any data dissemination as requested by research users who must currently 'remove and manipulate extraneous data'.

95. 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 and DWP) must end.

96. A non-commercial-use should be restored on data collected prior to changes of 2012 law which repurposed how data is used by new third-parties, because the Department for Education is liable for improper and unlawful re-use. Fifteen million people in the data had already left school and have never been told that their data could be used for the new purposes post-2012 and these re-uses are therefore in breach of data protection and wider privacy law.

97. The Department for Education should articulate a vision for education that moves away from controlling models of dataveillance, and instead prioritise local needs, using decentralised data for greater value across the sector at local level, and use sampling for national data purposes.

98. Data may reflect discrimination embedded in historic social, class and racial norms. Any historic data used in algorithmic decision making at national level (such as the standardisation model for exams or the LEO dataset) should be assessed with the benefit of hindsight from summer 2020 to identify and mitigate risk.

99. Commission an audit of systems and algorithmic decision making using children's data in the public sector at all levels, in particular where commercial machine learning processes education or children's social care, to ensure safety, fairness, accessibility, societal impact and sustainability are considered by-design in public policy.

100. Carry out a risk assessment of the planned 2021Children In Need (CiN) census expansion with a view to aggregate not individual data collection. The Unique Pupil Number (UPN) is routinely processed by thousands of companies daily, since the protections around its distribution were loosened in 2010. We believe that there has never been any assessment done on the risk levels this creates, in particular links between CIN data at Local Authority or national level and UPN distribution.

101. The Department must recognise the distinct issues raised in data governance and design mechanisms where personal data in a child's record may no longer be only personal data, but interpersonal, and about a whole household. The Department must be able to meet their legal obligations on access to records by the data subject including sensitive data (e.g., CIN census).

102. The Star Chamber Scrutiny Board (Department for Education data expansions decision making board) should increase public trust in their role in data collections after the

nationality/country-of-birth expansion 2016 crisis and start to publish its advance meeting topics, post-meeting minutes, summary of outcomes, and its Terms of Reference.

103. Every expansion of statutory data collections (school census and attainment) must have public consultation and Parliamentary scrutiny, ending the use of only a negative statutory instrument to introduce nationwide new or expanded children's personal data collections recognising that children merit specific protection with regard to their personal data.

104. Address the implications of poor data quality for policy making, research and operational re-use of administrative data in particular where used by other Departments, by ensuring transparency of each record to every person whom data is about on a regular (annual) basis or on demand so that people have the ability to correct errors in their own data held.

105. The data sharing approval panel (DSAP) meeting agenda, minutes and papers from project reviews and approval should be published, following the similar model of the UK National Statistician's Data Ethics Advisory Committee (NSDEC)[54].

106. Any recipient or user of national administrative datasets should be obliged to publish their work or outcomes of using the data in the public interest, free and open access. The public sector funds the creation, collection, linkage and cleaning of the data which companies then use for private-profit. A quid pro quo in return would be in the public interest.

107. Commercial users of the National Pupil Database must not continue to work around the safeguards in place in the 'five safes' research infrastructure used by academic researchers since 2018. Distribution outside this infrastructure, and resulting unsafe practice must end.

108. The DfE must act on the recommendations made by the UK Statistics Authority Office for Regulation in March 2018 including "publishing a public guide to data identifiability and the NPD either drawing on the identifiability spectrum framework developed by the Wellcome Trust Understanding Patient Data programme, or proving details outlining how the National Pupil Census and NPD will be GDPR compliant."[55]

109. Create a mechanism for an educational setting to download an individual's National Pupil Database record, at individual request, to let them see it, including to correct any inaccuracy and to inform them where data has been distributed. Schools should be able to download data reports either on demand, or a minimum annual basis. This would enable schools to show pupils what data is held about them, where it has gone, and allow schools to support the Department in meeting the duty towards national Subject Access Rights.

110. The Department for Education (DfE) must recognise individuals' and legal guardian existing rights to Object to Processing afforded in the UK Data Protection Act 2018 under the GDPR, and assess how this affects and will be met in their data processing of administrative datasets. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or fundamental rights and freedoms of the data subject.

111. Children must be given a right to restriction of disclosure to private companies to ensure their full development and adult flourishing by default. Individual school records with behavioural history should be suppressed from distribution; records such as violence, sexual misconduct, or drugs and exclusions. If these were a criminal record it would be suppressed under the Rehabilitation of Offenders Act 1974; but as non-criminal records, may be passed on for life to third parties, without a child's (or their later adult) knowledge, to an indefinite number of third parties.

[54] Published by the Office for Statistics Regulation https://uksa.statisticsauthority.gov.uk/?s=NSDEC

[55] UKSA recommendations to the DfE (March 2018) https://defenddigitalme.org/letter-ed-humpherson-to-neil-mcivor-2/

112. Start fair communications across the education sector with children and families, telling them annually which of their personal confidential data will be submitted before every school census and ensure the optional items and Right to Object are clearly communicated.

For Local Authorities

113. The basic consistency in how we count children across the education system must be addressed with process and technical fixes, through training staff and system design. A single census must always count either actual heads or full time equivalent, across a year or on a single day, not a mixed approach across different local authorities or Alternative Provision settings. (based on our research across every Local Authority)

114. Clear responsibilities and accountability for communication to families need to be established.

1.3.3.2 Findings 3 I Admin data collections and national databases

115. There are issues in practice of what data is collected, how it is collected and how those people are informed and able to exercise their rights in a meaningful way across the whole sector.

116. Our research indicates inconsistency in the collection of data about children in Alternative Provision, in the basics of how numbers were recorded. Some Local Authorities counted each child only once who spent any time in AP across the year no matter how often. Others counted the same child more than once if that child attended AP more than once in the year. Others counted the total full time equivalent across the year. Some counted children only in the AP setting on the day in January of the census. We suggest this basic counting problem should be considered and assessed in any reviews of "missing children."[56] We are not suggesting it is the cause of 'missing children' in the numbers, but we certainly think it is a contributory factor.

117. The majority of parents polled in 2018 do not know the National Pupil Database exists. 69% of parents replied to a 2018 poll that they had not been informed that the Department for Education may give away children's data to third-parties.[57] *"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."* (ICO, 2019)

118. The Department for Education policy supports unsafe data distribution and enables work arounds for commercial users to access children's identifying and sensitive records at scale.

119. Millions of children's sensitive personal confidential data at pupil-level have been released from the National Pupil Database in over 1,600 unique releases to third parties since March 2012.[58]

120. Repurposing of educational records has become normalised by the Department. Since July 2015 the Department for Education has facilitated the Home Office monthly matching of a total of 1545 children's national pupil records with Home Office records to find people for

[56] Freeguard, G. and Britchfield, C. (2020) Missing Numbers in Children's Services https://www.instituteforgovernment.org.uk/publications/missing-numbers-children-services

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

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

immigration purposes under a Memorandum of Understanding on data sharing[59]. Neither the DfE nor the Home Office demonstrate any accountability for the outcomes of what happens to children and their families as a result, saying in reply to Parliamentary Question 92745 in September 2020 that the information “is not readily available and could only be obtained at disproportionate cost.”

121. In 2019 the DfE permitted the use of 2,136 children’s records from the National Pupil Database for a criminal investigation. It is not known why this was not done by asking the school, but by using the national database.[60]

122. In April 2018 DfE permitted the use of the National Pupil Database for a DWP benefit fraud investigation of 185 children.[61]

123. The Department for Education in England is aware that they share too much data with third party users, calling it an ‘excessive’ amount of data in the underlying datasets’.[62] The DfE 2018 Hive data dissemination discovery report found that, “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.”[63]

124. Administrative systems that began 20 years ago are coming of age and questions of retention and destruction of individual education records now need both attention and action.

125. The necessary infrastructure on which safe, fair and transparent data processing runs in state education which ensures consistent good practice, understandable to the children, or even to school staff has never been built or is at best haphazard and has been retrofitted to the data distribution in practice.

126. A problem is caused at national level by school information management systems that do not offer local granular data controls. i.e. parents want ethnicity held by the school but not submitted in the national census.

127. Data collection systems can be far out of step with parental expectations. A data input form used by thousands of schools across England to record school census information in 2016 allowed administrators to ascribe a child's ethnicity. Italian parents complaints to the Embassy in London resulted in an apology from the DfE about country of birth and language forms sent out by UK schools asking parents whether their child was “Italian”, “Italian-Sicilian” or “Italian-Neapolitan”. The Ambassador pointed out that Italy has been a unified country since 1861.[64]

128. In 2015, a total of 37,000 students responded to UCAS’ Applicant Data Survey. 90% only agreed with sharing personal details outside of the admissions process only with active and informed consent[65]. This is ignored by the government and data users and there is no social contract for processing the Longitudinal Educational Outcomes (LEO) dataset or NPD linkage of Higher Education data.

[59] Home Office DfE datasharing MOU v1.0 in effect between 2015 and mid October 2016 when it was revised and reworded to remove “(Once collected) Nationality” the version 2.1 https://www.whatdotheyknow.com/request/377285/response/941438/attach/4/20151218%20DfE%20HO%20Final%20V0%201%20REDACTED.PDF.pdf

[60] Pupil data and Workforce data: Home Office and Policing data cooperation https://www.whatdotheyknow.com/request/pupil_data_and_workforce_data_ho#incoming-1630439

[61] ibid.

[62]Presentation to the NPD Bristol User Group 2016 by the DfE Data Modernisation Group

[63] 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

[64] BBC (2016) UK school pupil ethnicity question angers Italy https://www.bbc.co.uk/news/blogs-news-from-elsewhere-37631062

[65] 37,000 students respond to UCAS’ Applicant Data Survey (2015) https://www.ucas.com/corporate/news-and-key-documents/news/37000-students-respond-ucas%E2%80%99-applicant-data-survey

129. The Department for Education cannot continue to hold personal data collected between 2016-18 indefinitely that it does not use, because it was collected for Home Office not educational purposes (school census: nationality, country of birth). This requires regulatory enforcement of data destruction.

130. The Department for Education cannot continue to rely on research exemptions for indefinite retention of the National Pupil Database, since the same data is increasingly re-used for direct interventions and other incompatible purposes.

131. Research exemptions do not relieve such processing from all data protection obligations.[66]

132. Research use of data should not be considered 'neutral', may be used for interventions and may cause harm. A research project in 2013 through The University of Cambridge, the Greater London Authority and the Education Endowment Foundation (EEF) set up a randomised control trial to assess the effectiveness of an intervention for children at risk for fixed term exclusion from school in October 2013 with roughly 800 children in Years 9 and 10 in 40 selected schools. The NPD data requested was used to create a model to predict exclusion based solely on administrative data for London schools and schoolchildren. The trial was an independent evaluation of a 12-week-long intervention, Engage in Education-London (EiE-L), delivered by Catch22. "*Anecdotal evidence from the EiE-L core workers indicated that in some instances schools informed students that they were enrolled on the intervention because they were the "worst kids"; this may not only hinder any engagement in intervention but also jeopardise the teachers' relationships with the students and thus contributed to negative effects.*"[67]

133. The Department for Education passes the responsibility on to schools to explain to parents what data may be collected in the school census and what it will be used for. The DfE however does not pass on the full information to schools to allow the responsibility to be met, such as keeping secret Home Office re-uses. The DfE cannot tell a school which child's information was used in which third party release. Schools are therefore unable to meet this fairness obligation that the DfE delegates, and the DfE fails to meet its legal obligations.

134. Personal data about children is ascribed to them in schools, then gets added to their longitudinal records through the school census or attainment tests, and is kept forever. Children and parents never see their national school records. Mistakes that we do not see today, can get copied and distributed again and again, and used to make decisions by schools, companies, or other government departments.

135. The Department does not maintain records of the number of children included in historic data extracts[68] and it cannot tell individuals whether or not their data was sent to charities, commercial organisations, data analytics companies, journalists and think tanks, among the uses approved for research purposes. The DfE demonstrates little accountability for its own actions, when it comes to pupil data collected for the purposes of school accountability.

136. Sensitive data, special category data in data protection law terms collected in attainment tests is not given due attention in education compared to other sectors such as health. SEND data should be treated with the same respect as health data in the NHS. This is not currently the case and it is treated as routine administrative data. It is passed around apps companies and to platforms without parental knowledge or permission and to third-party researchers with too little attention. Where profiling includes ethnicity and disability or other SEN health related categories of data, it must be proportionate to the aim pursued, respect

[66] ADRN guidance for researchers http://www.adrn.ac.uk/media/1202/section_33_dpa.pdf 06/03/2016

[67] Obsuth et al (2016) London Education and Inclusion Project (LEIP): Results from a Cluster-Randomized Controlled Trial of an Intervention to Reduce School Exclusion and Antisocial Behavior https://link.springer.com/article/10.1007/s10964-016-0468-4

[68] Parliamentary written question - 109065 answered 23 October 2017 Pupils: Personal Records, accessed 2 April, 2018 https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-10-23/109065/

the essence of the right to data protection and privacy, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. (aligned with the GDPR Article 9(2)(g) Article 22(4)). Staff routinely process data on the assumed basis of a statutory obligation or duty in the course of a public task without understanding the nuance of obligations on special category data.

137. Data protection best practice is not always aligned with reasonable or ethical expectations of privacy. There is no opt out of the use of the National Pupil Database. The default public interest position in the UK is for sharing of public administrative data for secondary purposes is an opt-out, not opt-in mechanism, where one exists at all since the Digital Economy Act 207 (Troubled Families and Public Services) and Small Business Act 2015 (LEO data).

138. For children this is impossible where parents take decisions on their behalf which cannot be revoked. In education very little data processing is consent based. Children are entirely reliant on the decision making of the adults.

139. Pupil level data is produced by school staff at great workload cost, is passed on to the national databases from where it is distributed for free to commercial companies that repurpose it into for-profit products then sell it back to the same schools that created the data to start with, as data analytics back to schools with individually personalised profiles and targets for children.

140. Local Authorities are using data from Key Stage attainment tests and other pupil data for purposes it was not designed for. (See report of the project Data Scores as Governance: Investigating Uses of Citizen Scoring)) Data Justice Lab at Cardiff University. The researchers examined uses of data analytics in public services in the UK with a focus on re-use of administrative data. They are concerned with the advent of data-driven scores that combine data from a variety of sources as a way to categorize citizens, allocate services, and predict behaviour, by Local Authorities and their partner agencies. (Dencik et al, 2018).

141. Public engagement work carried out about public data uses has already been extensive, though it sometimes does not return the answers those who call for entirely new public engagement want to take into account. When the Administrative Data Research Network was set up in 2013, a new infrastructure for "deidentified" data linkage, extensive public dialogue was carried across the UK. It concluded in very similar findings as was apparent at dozens of care.data engagement events in 2014-15.[69] There is not public support for:

- *"Creating large databases containing many variables/data from a large number of public sector sources,*
- *Establishing greater permanency of datasets,*
- *Allowing administrative data to be linked with business data, or*
- *Linking of passively collected administrative data, in particular geo-location data"*

140. The other 'red-line' for some participants was allowing *"researchers for private companies to access data, either to deliver a public service or in order to make profit. Trust in private companies' motivations were low.*

141. The Department for Education has not yet delivered on recommendations made by the UK Statistics Authority Office for Regulation in March 2018 including publishing a public guide to data identifiability and the NPD" drawing on the identifiability spectrum framework developed by the Wellcome Trust' Understanding Patient Data programme, or proving details outlining how the National Pupil Census and NPD will be GDPR compliant*.[70] (*See also ICO 2020 compulsory audit when the NPD was found not to be GDPR compliant.)

[69] Administrative Data Research Network Public Dialogue (2013) https://defenddigitalme.org/dialogue-on-data-exploring-the-publics-views-on-using-linked-administrative-data-for-research-purposes/

[70] Letter from the UK Statistics Authority Office for Regulation to the Department for Education (March 2018) https://defenddigitalme.org/wp-content/uploads/2020/09/Letter-Ed-Humpherson-to-Neil-McIvor.pdf

> The Commercial department do not have appropriate controls in place to protect personal data being processed on behalf of the DfE by data processors.
>
> 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.

The ICO, October 2020
Department for Education data protection audit report
Executive summary on DfE national pupil data handling

1.3.4.1 Recommendations Four I Principles and practice using technology today

We are yet to see articulation of a future-thinking vision for education that moves away from centralised data surveillance and intra-schools competition, and instead prioritises local needs and collaboration. The best of what COVID-19 highlighted in communities across the UK was in systems of human support networks, with the continuity of learning and children's welfare and rights at its centre. In June 2019, the High Level Expert Working Group on Artificial Intelligence (HLEG-AI) in their Policy and Investment Recommendations for Trustworthy Artificial Intelligence, proposed children must be better protected when using emerging technologies. That needs extended in England to protection from excessive or non-consensual research trials of emerging products and practice. (See case studies, part three)

For policy makers at all levels

142. Technology must first do no harm through its application or through a denial of provision. The digital environment in education must serve children well. It must be safe, inclusive, and equitable, promoting social justice and human dignity.

143. Children in England require adequate online infrastructure to support digital access as part of remote learning in state education. This is a priority in COVID-19 but of equal urgency for every child and homework under regular circumstances.

144. Access to hardware and software in the classroom is important to provide and fully fund across education. State education must offer a fully funded, interoperable infrastructure that does not rely on parent paid or leasing schemes to spend hundreds of pounds in order to have access to hardware in the classroom. No child in state education should have to pay for the technology that a school requires them to use. Access must be across education, including for example further education to enable skills training and the access to specialist software such as in design and engineering.

145. Investment is necessary in people and pedagogy, through Initial Teacher Training and Continuous Professional Development. Data privacy and protection and data and digital skills, and a review of current policy and practice should begin through consultation.

146. A regional shared-service model for legal and data protection due diligence and contract support is needed to reduce staff workload and increase standards. Build national and regional knowledge and support centres to carry out due diligence research and reduce the investigative burden for school staff in procurement with modified public tasks, that can have the clout at scale to modify contracts with companies but with reduced commercial and competitive incentives seen in today's Grids for Learning infrastructure. They must be transparent and accountable to the public, subject to FOI and publish registers of procurement, together with associated due diligence assessments, DPIA and audits.

147. Create safeguards for children from the use of excessive and invasive surveillance via various biometrics, facial detection and recognition, emotional manipulation, and neuro-/cognitive technology by commercial companies, or via webcam, voice recording, or gait and movement analysis, noting UN Special Rapporteur David Kaye's call for a moratorium on facial recognition technology.

148. A statutory ban is needed on webcams taking a photograph of a computer user without their knowledge or permission, and on monitoring their use of the Internet or school digital environment at individual user level with personalised risk categorisation outside school

hours. Monitoring should be kept distinct from security, filtering and blocking services and not at pupil level activity.

149. Pupils and students must be free from any obligation of using personal profiles and accounts on social media to sign up to apps used for school work.To avoid privacy risks, educators must allow Higher Education students to separate group and personal accounts and more broadly, limit their use for course communications and administration.

150. Artificial intelligence and other emerging technology companies must not exploit children's data gathered in the course of compulsory education, for their own company product development. Companies must not use AI as a loose marketing term, when a product does not contain any computing that can be classed as artificial intelligence. (See case studies, part three)

151. Alternative ways of meeting a child's right to education should be met without detriment if a child or either parent objects to participation in product trials following a similar consent model as biometrics in schools in the Protection of Freedoms Act 2012. Routes for redress and the accountable owner for outcomes must be a named individual, communicated in advance of the start of a trial and not only the third-party organisation company name.

152. Following the HLEG-AI recommendation, children should be ensured a free unmonitored space of development and upon moving into adulthood should be provided with a "clean slate" of data storage by default with retention beyond compulsory education in administrative datasets, on a necessary and proportionate legal basis, as an exception not the rule.[71]

1.3.4.2 Findings 4 I Principles and practice using technology today

153. A vision for education should include how technology is a supporting tool, not a decision-maker shaping the design and delivery of education. The current edTech bolt-on product approach from the top-down, or even through recommender 'Roadshow' schemes will not deliver that vision, because it is based on product-centric promotion, not a child-centric, skills and capability strategy. A shift is needed from edTech promotion to how and why education should use which technology at all in the curriculum not just to support school admin. Whether what is really needed from the child's perspective exists in the market today at all should be assessed as part of reviews into lockdown learnings. If not, then build it.

154. When it comes to children's learning what is current edTech promoting that is not centred on testing rote knowledge? Where is the adaptive learning edTech that is truly personalised and respects privacy not done through company-centralised surveillance? Where is a strategy driving collaboration and creativity, the Renaissance skills that go beyond regurgitating knowledge about how to apply critical thinking skills to analyse and synthesise content? Much of the edTech focus is on school administrative and teacher workload support. While that may result in better businesses, it won't get better outcomes for children.

155. For an edTech strategy across England that works for all, investment in people, pedagogy, and local infrastructure should not be focussed on further embedding the market power and hold over the sector of big tech monopolies, or for-profit individual companies ad hoc promotion that then frequently get bought out by venture capital. Knowledge generated by edTech about learning from our public sector, should not be indefinitely siloed and monopolised in competitive companies. Private sector companies should, with proper

[71] Policy and Investment Recommendations for Trustworthy Artificial Intelligence (accessed July 1, 2019) (published June 26, 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)

privacy preserving techniques, ensure open data in a quid pro quo exchange that is of benefit at local level.

156. Technology should not be a means in itself and the edTech agenda needs to recognise that technology may not offer appropriate solutions in particular to complex social problems. "*To what extent is 'intelligent' surveillance a solution for anti-social youth behaviour in an area without enough alternative evening activities or public spaces? The focus should be on taking off the 'tech goggles' to identify problems, challenges and needs, and to not be afraid to discover that other policy options are superior to a technology investment*." (Veale, 2019).[72]

157. Communities have kept it together in the face of COVID-19 and it is communities with schools at their centre that will bring us out the other side. Schools have found approaches to managing ongoing blended learning, and raised financial support for their most vulnerable families, often anchored by local business loyalty, where the DfE provision has let them down. We will continue to need that resilient human network after we leave the EU. Youth services need restored.[73]

158. Staff working in a school digital environment lack consistent levels of support from people with technical competence (regional overarching support has been reduced since closure of British Educational Communications and Technology Agency (Becta)[74] and austerity cuts in Local Authorities in shared services.

159. 'Free-to-school' products may be popular with schools scraping by on austere budgets, but can come at a cost to a child if personal data is collected and used by the provider in ways a family cannot see. If we change nothing, children and parents will never know the extent to which their personal data has been shared, used, misused, sold, breached, or hacked over the course of their school lifetime and they will not be able to exercise their rights as an adult, leaving school at 18. Harms are not all theoretical or in some far off future.

160. Safeguarding-in-schools services and software can be deeply invasive. Legislative protection and policy change are needed to accompany the existing weak statutory guidance in England for school pupil web surveillance vendors, to assist schools to comply with the Data Protection Act 2018, human rights law, breach of communications law, and to end the serious invasions into private and family life that exist today which have become normalised through overreach in school practice, in particular outside school hours.

161. Highly sensitive biometric data is a child's for life. It may be used in a child's adult life for as yet unidentified significant security and identification purposes, yet biometrics may be used rather casually in schools for insignificant tasks such as printer management. Based on FOI responses carried out by Pippa King in 2018, 57% of 400 schools asked, used a biometric system, and 37% used biometrics for more than one application. Our commissioned poll of 1,004 parents[75] in February 2018, found that 50% had not been informed for how long a child's biometric data would be retained. Parents don't know how companies use children's data from school; from homework apps, the school census, to CCTV. Only half of parents say they have been told how long CCTV images are kept for. Biometrics has grown exponentially without any corresponding increase in the regulation or oversight who can collect such sensitive data and why. Discrimination against those who opt out of its use in

[72] Veale, M. (2020). A Critical Take on the Policy Recommendations of the EU High-Level Expert Group on Artificial Intelligence. European Journal of Risk Regulation, 1-10. doi:10.1017/err.2019.65

[73] Puffett, N. (2020) Children and Young People Now | Spending on youth services has been cut by nearly £1bn in real terms in the space of eight years, the latest analysis of local authority figures shows.https://www.cypnow.co.uk/news/article/youth-services-suffer-1bn-funding-cut-in-less-than-a-decade

[74] BECTA closure announcement | DfE to close arm's length bodies to improve accountability
(2010) https://www.gov.uk/government/news/dfe-to-close-arms-length-bodies-to-improve-accountability

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

canteen services or lack of respect for rights protected by law are already common. Further data about social, emotional, and mental processes may not fit the data protection definitions of use for the purposes of identification of an individual.

162. Punitive examples of poor edTech products are mean spirited, invasive and treat children as outliers in behavioural norms or as a potential criminal, cheat, or fraud.

163. Everyday problems parents bring to us, can range from disputing of the value of a maths app that makes so much of the gaming aspects of its animation that a child is stressed by not being able to do the sums fast enough so that sheep fall off a cliff, to feeling bullied through the behaviour profiling app that the teachers use to award positive or negative points in front of peers in the classroom to the point that a child dare not say anything at all.

164. A vast array of school software is premised on detailed and centralised data surveillance. Not only what did you spend in the canteen today, but what exactly did you buy? How did you behave today? Who were you sitting next to when that happened? When were you out of school and what were the reasons for it? Information that trusted teachers have always known and used to put a child at the centre of their teaching and care, are now used out of context and may be accessible to hundreds of strangers including across a school Trust, companies or researchers. Pupil data has become business intelligence used to define school improvement or metrics with which to measure school standards. Simple facts have taken on interpretations and weight with a permanency they were never intended to have.

165. Industries have been built around reporting to parents to a degree and complexity many do not need or want, producing detailed school data analytics at pupil level and around creating insight that the pupils may not benefit from, or when simple information would be enough.

166. We are not aware of any independent research into what parents want and the quality of information such tools convey.

1.3.5.1 Recommendations Five I EdTech evidence, efficacy, ethics, exports engagement

Policy makers should recognise that the hype of ‘edTech’ achievement in the classroom so far, far outweighs the evidence of most delivery. More than three quarters (79%) of teachers and school leaders surveyed want to see clear proof that EdTech works in the classroom. To build a trusted relationship in edTech efficacy and intentions, then a sea-change is needed in industry, research, Think Tank and policy making bodies current approach and attitudes that assume entitlement to access state school children, trial products on them, and use their data as a free resource. Normalised poor practice should be reset, enabling safe and ethical product development, that is not exploitative or encroaching on educational time, supported by common standards developed in conjunction with children and families, their representatives, civil society, industry, teachers, and regulatory bodies.

Evidence

167. Independent assessment of the Nesta / DfE £4.6m partnership Innovation Fund interventions[76] should be undertaken considering lawful obligations towards data processing, due diligence and of children’s rights for both consent to participation in and in the data processing aspects of edTech research trials and innovation fund interventions in England.

[76] Department for Education / Nesta EdTech Innovation Fund. This project started in April 2019 and will end in December 2021 https://www.nesta.org.uk/project/edtech-innovation-fund/

168. Oversight and accountability is required of all product and research trials intended to gather edtech evidence in a consistent single view. Testing products in 'real' conditions in educational settings, may be extremely hard, but it should be. Our children do not go to school in order to be research trial participants or perform school work in order to perform labour to develop a commercial product. The state has a duty to meet a child's right to education and with their best interests at heart without exploitation or unduly manipulating their behaviour or affecting learning in ways that a child cannot see or choose. Some research trials and product trials today have inadequate ethical oversight and this must be addressed with urgency. (see 1.3.9 Research)

Efficacy

169. Democratic sector-wide consensus is needed at least on some aspects of state education and technology. Competing discourses will continue to debate personalised learning and contested meanings about the type of expertise is needed for the 21st Century. What self-directed learning should look like? Whether education is about process or content? And the type of evidence that is required to establish whether or not personalised learning leads to better student outcomes?[77] We cannot continue to ignore the reality that these products are in use, siloed, rarely serving children or families' best needs first, and poorly regulated.

170. Recognise that not everything that looks or sounds good, may be good and efficacy and ethics of aims, need assessed. "In educational systems that emphasize development and, for example, social competences, formative assessment might be higher on the list. As a result, there is a risk that AI might be used to scale up bad pedagogical practices." (Tuomi, 2018)

171. While the EdTech Evidence Group[78] (EEG) organised by Sparx aims to "*sustain high-quality evidence gathering in members' own organisations*," it lacks independence and whilst its members integrity is not in doubt, externally it can only be seen to be marking its own homework. This function could be better placed on a statutory function under the new data guardian and ombudsman for children's rights in education, and would play a role in ethics, exports and give guidance on engagement between the sector, children, families and educational settings in matters that go beyond the remit of data protection at the ICO.

Ethics

172. Transparency should also start from the top down. Public transparency and accountability of the edTech influencers seeking to shape the sector should be encouraged through publication of meeting minutes and Terms of Reference from governmental and non-governmental bodies including the DfE EdTech Leadership Group[79] and the edTech Advisory Forum[80] and the edTech Evidence Group, to enable wider democratic discussion.

173. Ethical use of AI in the classroom needs addressed in legislation and a Code of Practice. Recognise that some emerging technology is inherently harmful to the dignity and human rights of a child and should be banned from UK education.

174. Enable children to have a free unmonitored space of development and upon moving into adulthood with data deletion by default to provide a "clean slate" of any private third-party

[77] Regan, P and Steeves, V. (2019) Education, privacy, and big data algorithms: Taking the persons out of personalized learning https://doi.org/10.5210/fm.v24i11.10094

[78] The EEG brings together leading UK EdTech companies who share a belief that there needs to be a step-change in the level of evidence available about EdTech https://www.edtechevidence.com/

[79] Snowdon, K. (2019) Schools Week | Paralympic swimmer Chris Holmes will chair a new expert group to help improve the use of technology in schools. https://schoolsweek.co.uk/paralympic-swimmer-to-chair-new-edtech-expert-group/

[80] Booth, S.(2020) Schools Week "Independent review to probe ed tech sector's response to Covid-19" https://schoolsweek.co.uk/independent-review-to-probe-ed-tech-sectors-response-to-covid-19/

storage of data aligned with the HLEG-AI recommendations. Schools should retain any necessary records as controllers, not companies as data processors noting the DfE guidance on unique pupil number (UPN) retention and its requirements to lapse.

175. Safe use of AI and big data analytics by state and commercial sector in education needs stronger enforcement of responsibilities and rights on data processing, and in particular minimising profiling, and higher risk processing of biometric data used for identity systems to process basic administrative tasks in the canteen, library, locker and building access.

176. Advertising should not be considered a compatible purpose under data protection law, that overrides a child's best interests, or the protections of rights and fundamental freedoms. Advertising to a child and/or parents should be banned in education (edTech) products.

Exports

177. For a successful UK export market, any makers and manufacturers of edTech must ensure to meet the full range of widely recognised international children's rights conventions, legislation and guidance in order to find receptive markets and regulatory acceptance outside the UK. These standards should be consistent and clear across the domestic sector to ensure fairness for all and become a benchmark for high quality expectations.

178. UK international reputational risk must be protected. If the UK government hopes for edTech exports are to become a reality, we must champion safety, quality and pedagogical benefit in the home market. Without this, reputational risk will not only affect single products abroad, but contaminate the UK reputation for export as a whole.

179. The knock on effects of changes intended elsewhere in government must be appreciated in their effect on edTech export of children's products. If the UK gains a reputation for disdain of human rights[81], the edTech exports sector will undoubtedly suffer not only in terms of sales impact to schools, but in the likely impact of loss of a data adequacy decision.

180. Any national promotions such as the BESA LearnEd roadshows which have an indirect Department for Education approval, should have an independent assessment process to ensure high standards of data protection and ethics in the products being promoted.

Engagement between companies and in educational settings

181. Procurement decisions should only be made after thorough due diligence of financial, ethical and legal policy and the experience for children using products in practice behind the screen and in consultation with families at the educational setting.

182. The controller/processor relationship needs redrawn in practice in edTech adoptions and engagement with families is necessary in order to be able to address rights. There are serious data implications: for inequality, costs, privacy and surveillance. Contract terms must be possible to adapt at school level and for example, end the bundling of multiple and bundled processing purposes into the contract such as repurposing for third party research for which the processor becomes a joint data controller, diminishing the school's control over records. Today's terms and conditions often go beyond processors' lawful basis that is not extended to them through schools' public task.

183. A National Guardian for education and digital rights, would provide a bridge between companies and educational settings and families, with a focus on people rather than products. Its role may support due diligence and ethical approvals of products but for the purposes of the protection of children's rights, rather than product promotion. There is currently no infrastructure to support schools or families with standards, oversight or accountability. Capacity and capability would benefit from a cascading network of knowledge with multi-way communication, along the lines of the NHS Caldicott Guardian model.

[81] The Sunday Telegraph front page (September 13, 2020) https://twitter.com/BBCNews/status/1304893718084886530?s=20 Johnson set to opt out of human rights laws

Fig 2. An illustrated day in the life of a datafied child l common school activities

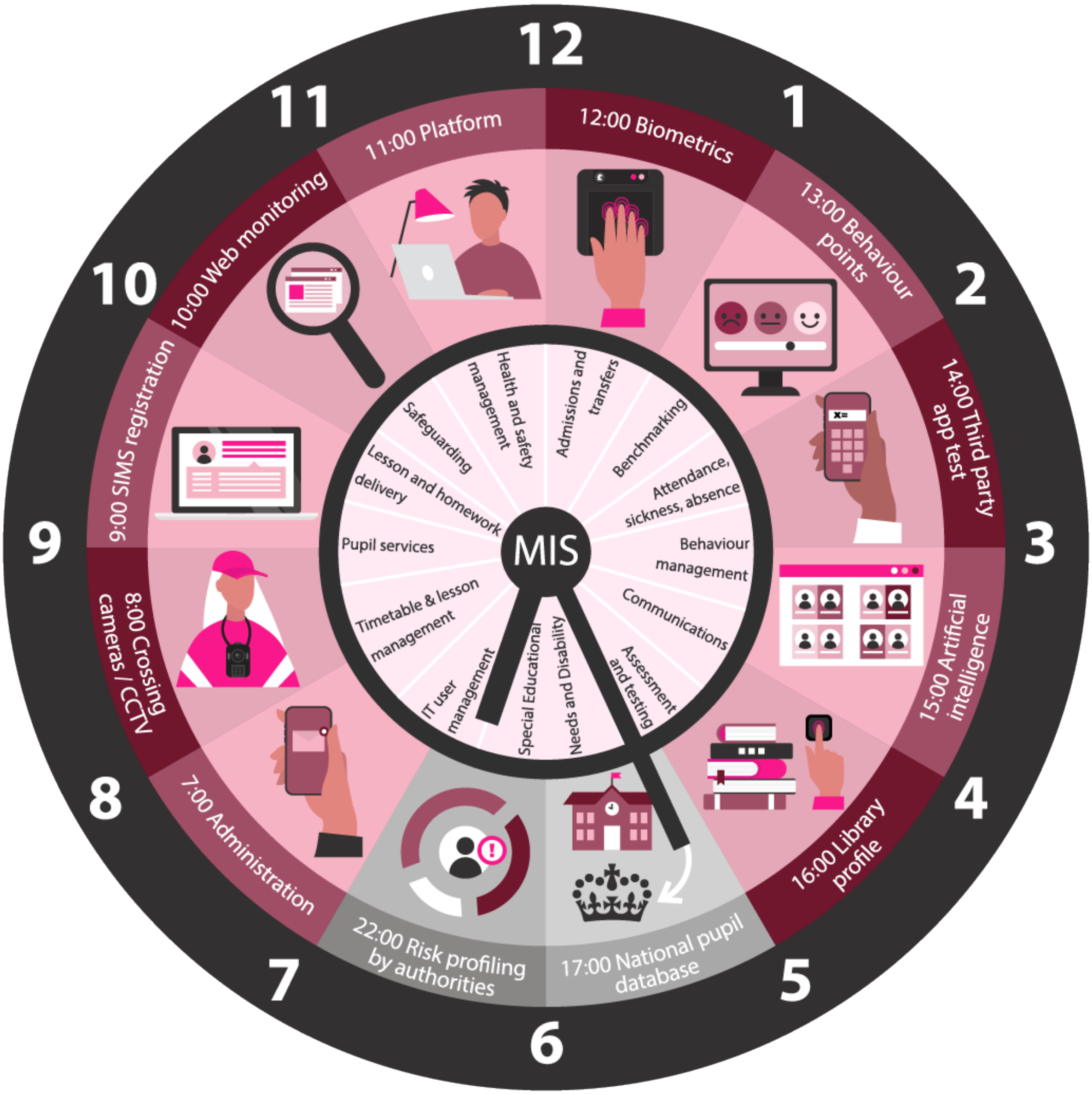


Fig 2. This illustration is intended to show a high level digital day-in-the-life of an eleven year-old at state secondary school. The common core administrative functions in educational settings that are supported by the Management Information System, the digital centre of a school records system. The outer ring are the activities in which children's data most commonly leave the school and are processed or controlled by third-parties for daily interactions. It also includes the processing of hours that children do not see: data transfers to Local Authorities and the Department for Education as part of regional decisions on risk scoring and predictive analytics programs, or for the national census termly for the school census and annually for some others. These functions may entail processing of a child's personal data by dozens of companies in one day, every day, across their entire education. Most of this processing will be done offsite, on other companies' servers (cloud based data storage) and no longer retained only on the school premises.

1.3.5.2 Findings 5 I EdTech evidence, efficacy, ethics, exports, engagement

Evidence

184. At local level, UK research published by the learning technology company Sparx, shows that more than three quarters (79%) of teachers and school leaders want to see clear proof that EdTech works in the classroom.[82] Sparx reported that UK schools spend about £900m on education, technology with the UK EdTech market set to be worth £3.4bn in 2021.

185. Most importantly the EEG points out that there is a need to have "*efficacy and educational outcomes at the heart of our product development*" and that schools need to have consideration of their 'opportunity cost': a year spent using the wrong product for that customer means a year's missed opportunity for their students or staff.

186. But how is any negative effect on a child who spends a year using the wrong product resolved? The harm that bad technology does to young people in educational settings should be the problem we solve first. Some of the current and emerging products may be at best ineffective and take away teaching time without additional harm. Others are used to punish or shame children in front of peers, or scoring can be used to ration resources.

187. The emerging calls for independent evidence in edTech are welcome, but are not enough to protect the sector when one of its own falls short, and whether through misleading marketing or unlawful and unethical practices, a company causes widespread backlash or mistrust in the sector.

Efficacy

188. The impacts of technology use on teaching and learning remain uncertain. Andreas Schleicher – the OECD's director of education – caused some upset in 2015 when suggesting that ICT has negligible impact on classrooms. Yet he was simply voicing what many teachers have long known: good technology use in education is very tricky to pin down. (Selwyn, 2019)

189. Remote learning under COVID-19 has demonstrated both how technology may support learning but also revealed edTech shortcomings at first hand in the experience of many parents.

190. Machine learning in children's social care may have dangerous blind spots. Deciding what shape future societies will take, not only involves determining, democratically and inclusively, how to steer the values and motivations that are currently driving the gathering energies of technological advancement in machine learning. (Leslie et al. 2020). It requires an understanding of how children are being shaped in their use of and use by technology today. Technology and its infrastructure is not politically, ethically, or economically neutral.

Ethics

191. *"Some of these e-learning platforms and the learning analytics they facilitate have enormous capacity to foster the development of innovative and effective learning practices. At their best, they can enhance and complement the interactions of students, parents and educators in the educational environment and help them fulfil their respective potential. Nevertheless, e-learning platforms may pose threats to privacy arising from the collection, use, reuse, disclosure and storage of the personal data of these individuals."* (ICDPPC Resolution on E-Learning Platforms, 2018)

[82] Sparx https://sparx.co.uk/eeg-new-research/

192. There need be no conflict between privacy and innovation, yet some products in emerging fields, including machine learning and Artificial Intelligence infringe on rights. Legal guardians in the UK are concerned according to Nesta, how this may affect their children including through discrimination and social equity. (2019)[83]

193. 61% of parents polled by Nesta for the report Educ-AI-tion rebooted?, anticipate that AI will be fairly or very important to the classroom in the near future. However, many are fairly or very concerned about consequences of determinism (77%), accountability (77%) and privacy and security (73%).

194. The current postcode lottery of product trial participation and adoption across the sector, a single school and a child's school lifetime, means thousands of children are treated unequally and are guinea pigs in the government agenda to develop an edTech market.

195. *"Edtech is often not informed by pedagogy and the design of interfaces often lack user-centricity, putting hurdles in the way of teachers, rather than empowering them."* (Aerts, Educ-AI-tion rebooted? 2019)

196. New and emerging technologies are increasingly invasive and need greater ethical attention. A wave of advocacy for neurotechnology development and implementation is spreading in the field of education. (Williamson, 2018d)

197. Southgate et al point out in their 2019 report Artificial Intelligence and Emerging Technologies in Schools, commissioned by the Australian Government, that: *"Luckin and colleagues (2016) also identify the potential for AI teaching assistants to be used to unfairly or surreptitiously surveil the performance of teachers (using pupils' data), a point supported by Campolo et al. (2018) who recommends that 'more research and policy making is needed on the use of AI systems in workplace management and monitoring' (p.1). Other concerns include the way in which AI aims to change learning behaviour through making recommendations, using persuasion and offering feedback, which may not ultimately be in the best interests of the learner. There are some who suggest that AI learning companions that are intended to support students on their lifelong learning journeys 'may result in the perpetual recording of learner failure to the detriment of future progress.'* (Luckin et al., 39).

198. Safe data and ethical practice with clear explanations for families must be prioritised by design and default. Companies must demonstrate that they meet the requirements of the rule of law not simply state it in privacy policies. Companies must stop using pupil data for their own purposes for profit, or to make inferences about autism or dyslexia for example, if that's not your stated product aim, it's likely unlawful. Contract terms for settings must be careful not to burden schools with long term technology choices made in the short term and control of vendor relationships and activity must remain with the setting.

199. If a school chooses to participate in a research trial or government department driven intervention, it may receive £1,000 for its administrative costs. These incentivise schools to say yes but children often have no way to refuse. This power imbalance must be addressed through an opt in mechanism and equal alternative activity offered without detriment.

200. There is no independent overall ethical oversight of these trials and the sector at scale at a national level, or duty to publish evaluations for parents of previous trials of the same product to be run in their school to make an informed decision about risks and benefits.

[83] To obtain the perspective of parents on AI and education Nesta commissioned YouGov to undertake a survey of 1225 GB parents with children aged 18 and under https://media.nesta.org.uk/documents/Future_of_AI_and_education_v5_WEB.pdf Educ-AI-tion Rebooted? Exploring the future of artificial intelligence in schools and colleges

201. In 2017 Wired magazine[84] revealed that the government's Behavioural Insights Unit had been experimenting with using machine learning algorithms to rate how well schools were performing, and they were described in ways that seemed opaque by design: *"Data on student's ethnicity and religion were deliberately excluded from the dataset in an effort to prevent algorithmic bias. Although some factors will influence the algorithm's decision more than others, Sanders refused to say what those factors were. This is partly because he doesn't want schools to know how the algorithm makes its decisions, and partly because it is difficult to know exactly how these algorithms are working, he says. "The process is a little bit of a black box – that's sort of the point of it," he says."*

202. Technology can be transparent, decentralised, collaborative and user-focussed. Privacy preserving tools can be built that do not require registration and still be free, they can run directly in your browser without data retention.[85] Most popular UK used tools are not like this, but if such standards were mandated then it would level the playing field for participants that choose to avoid today's data surveillance and adTech-based services.

203. Ethical use of AI in the classroom also needs to consider what authority and perception of a single truth assistants such as Alexa, Siri or Cortana offer. These systems are not designed with children in mind, and their vocabulary and interactions may be unexpected. In February 2018 Alexa users reported their machines emitting unexpected laughter-like and whistling noises without being prompted to wake.[86]

204. How will children know that an electronic assistant merely offers the top answer that a search engine would do in response to a question, but without the ability to cross reference that answer with others. How will children critically evaluate answers offered by the computer with a human-like voice interface, if there is no alternative on offer to evaluate against? Or will they understand that any list of answers has been pre-determined by the design of the search engine corporation and their in-built values, or lack, and bias of importance and rankings.

205. Professor Laura Czerniewicz is the Director of the Centre for Innovation in Learning and Teaching (CILT), at the University of Cape Town wrote in 2020,[87] *"What we learnt from going online during the university shutdowns in South Africa is that it will be political. Change will be appropriated for different ends and tell different stories for different people. Technology is never neutral. Keep it simple and as complex as is essential. Keep issues of inequality upfront. Plan for your own context. There are serious data implications: for inequality, costs, privacy and surveillance. It is not just academics and students who are under pressure, remember all the other people involved. Be careful not to get stuck in the long term with technology choices made in the short term. Keep academic control of vendor relationships."*

Exports

206. The Department for Education (DfE) and Department for International Trade (DIT) launched an International Education Strategy in March 2020. The strategy sets out the government's ambition to increase the value of education exports to £35 billion per year by 2030 and suggests almost a quarter of Europe's education technology companies are based in the UK. The April 2019 edTech strategy stated that EdTech exports are worth an estimated £170 million to the UK economy.[88]

[84] Reynolds, M. (2017) UK's Nudge Unit tests machine learning to rate schools and GPs https://www.wired.co.uk/article/nudge-unit-machine-learning-algorithms-schools-ofsted-doctors-behavioural-insights

[85] Meetzi is a Jitsi-based tool, operated by LimTec GmbH in Germany https://klassenzimmer.meetzi.de/

[86] Liao, S. (2018) The Verge, Amazon has a fix for Alexa's creepy laughs https://twitter.com/i/moments/971424274731950081

[87] Czerniewicz, L. (2020) What we learnt from "going online" during university shutdowns in South Africa https://philonedtech.com/what-we-learnt-from-going-online-during-university-shutdowns-in-south-africa/

[88] EdTech Strategy marks 'new era' for schools (April 2019) https://www.gov.uk/government/news/edtech-strategy-marks-new-era-for-schools

207. While the edTech sector may have enjoyed a lack of regulation enforcement in England to date, companies cannot expect similarly soft approaches from other countries, in particular where data protection supervisory authorities are more active in the education sector.

208. Despite this when we asked at the BESA LearnEd roadshows in 2019, BESA had not carried out data protection risk assessment as part of any due diligence in the products it was promoting.

Engagement

209. Often tech 'solutionism' simply shifts an existing process from paper to computer but fails to cater for structural disadvantage or becomes more discriminatory or creates new risks such as cashless systems[89].

210. The proliferation of competitive apps and platforms in use create a siloed set of tools that parents must navigate between for a variety of different purposes; for home school communications, administration of cashless payment systems, booking appointments, recording absence, helping children to do or submit homework. This increased time and effort is pushed onto parents, compared to when none of these digital tools were previously available. Most of the communication through these systems may be one way because the administrator from the school is not the department responsible for the area; questions on welfare, communications or academics.

211. We have found no research on the parental experience of digital tools; how time consuming parents find it to manage multiple different processes on different apps in addition to emails, push notifications, letters and information posted on the school website or whether these tools offer time savings to schools or displace the admin time required to parents.

212. A consistent approach is needed for school children, students or their families to be fully aware of how their data are being used, and in the course of state education they have no meaningful choice or control over data processing. We believe few staff in institutions across the state education sector, providing services to children aged 2-18, have adequate grasp of this. This is a poor foundation for the expansion of an edTech strategy DfE began in 2019. This needs developed in conjunction with stakeholders and expectations set in legislation.

213. Complexity is no excuse for failing to provide information to the child or family.[90]

1.3.6.1 Recommendations Six I Children's rights in a digital environment

Devolved nations have made greater efforts than England to establish a national child rights framework across public services delivery. (Wales 2011 Rights of Children and Young Persons Measure and in Scotland the Children and Young People's Act 2014). To strengthen a unified and outward looking approach to children's rights would bring consistency across the Union for business and the public sector with a more sustainable and explainable standardised set of expectations.

For policy makers at national level

214. All stakeholders must recognise that children have rights in the digital environment that may be different from an adult. From the static point of view the child is a person who has not yet

[89] The Register (2020) Wisepay 'outage' is actually the school meal payments biz trying to stop an intruder from stealing customer card details https://www.theregister.com/2020/10/07/wisepay_outage_was_cyber_attack/

[90] Article 29 Working Party 29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2017) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

attained physical and psychological maturity. From a dynamic point of view the child is in the process of developing to become an adult. (WP29, 2009)

215. The government should level-up a duty to undertake the assessment of child rights impact in its own and wider public sector functions to the highest current standard across the devolved nations. Have due regard for part one of the UN Convention on the Rights of the Child and its optional protocols to which the UK is a signatory state. Child Rights Impact Assessment should be obligatory as part of large scale technology and/or data project introductions. Data minimisation, purpose limitation, and data retention should be given additional weight in data project planning, system design, practice, and enforcement when dealing with a child to ensure children’s flourishing and development to their full potential.

216. Commit to children’s rights in education; to access education, to equal treatment, to participation, reputation, to privacy of communications and family life, to freedom of speech, and to the full and free development and human flourishing at the centre of any technology in a world in which decision-making about us, is becoming ever more machine led without us.

217. Recognise that children’s full development and flourishing may be supported but may also be limited by data about them; through labels given to them for life or their digital footprint compromised in school, or through the use of historic educational records used in predictions or for data-led decision making using individual level data, or as part of a data cohort.

218. The State has obligations to meet in its lawmaking and procurement at all levels of government to respect the UN General comment No. 16 (2013) on the impact of the business sector on children’s rights. This needs applied in practical ways and through legislation, Statutory Guidance or enforceable Codes of Practice.

219. General comment No. 5 on the implementation of the UNCRC emphasises that *“implementation of 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, thus creating indirect obligations on such business actors.[91] (UNCRC, 2003)

220. Recognise all obligations in Article 24 in the Convention on the Rights of Persons with Disabilities regarding education.[92] These duties apply to all children, with a view to realising this right without discrimination, and on the basis of equal opportunity.

221. Article 12 of the UNCRC promotes the child’s right to express his or her views freely, “in all matters affecting the child”, those views being given due weight. The government must enable standardised tools and routes to exercise rights under data protection law principles, the right to information, the right to participation, and the right to privacy and family life; engaging the child as an active participant in the promotion, protection and monitoring of his or her rights, when it comes to a child’s journey through education and control of their digital footprint.

For the Department for Education

222. Build the infrastructure for an improved alternative model of data rights’ management in education, as an addition not instead of individual empowerment, styled on that of the U.S.,

[91] General comment No. 5 on the implementation of the UNCRC (2003) http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsiQql8gX5Zxh0cQqSRzx6Zd2%2FQRsDnCTcaruSeZhPr2vUevjbn6t6GSi1fheVp%2Bj5HTLU2Ub%2FPZZtQWn0jExFVnWuhiBbqgAj0dWBoFGbK0c

[92] Convention on the Rights of Persons with Disabilities (CRPD) Article 24 https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/article-24-education.html

governed by national law, the Federal Education Rights and Privacy Act, FERPA with regional controls and oversight, to better control national, regional and local data rights.

223. Subject Access Rights must be met by all government departments, including the Department for Education and its arms length bodies, and through easy to access routes.

224. Uphold the dignity and the rights of children with disabilities through the guaranteed award of an Education, Health and Care Plan upon application.

225. The necessity and proportionality of the permanent national pupil database and Individual Learner Records should be audited with regards to 'sealed envelopes' for children at risk or for whom a permanent identifier will carry over an old name or identifiers that put any child with a new identity or location at risk.

226. Enable better protection for vulnerable children through suppression of behaviour and exclusion records for children, treated similarly to the Rehabilitation of Offenders Act 1974.

227. End state surveillance under the Prevent Programme, stopping the mass monitoring 24/7 of pupils' digital activity, collection of communications data, or retention of records over time of individual behaviour by companies, in particular any data storage abroad should be deleted.

For educational settings and companies they use

228. Educational settings should always remain data controllers. Companies that process pupil data not for the purposes a school requires, but the purposes decided by the company (product enhancement and new development, research, data analytics) should ensure they understand the implications that may change them from a processor to a controller and realise this is not determined by terms and conditions, or what is stated in a contract, but by the nature of the data processing. Companies alone cannot make decisions about how or why data should be processed, those instructions must be governed from the educational setting, during the pupil school life and beyond.

229. Companies that process children's data should publish an annual child-friendly / plain English policy of use and register of any data sharing between or outside its own business

- international conglomerates with multiple affiliates that may include any other subsidiaries, joint venture partners or other companies that they control or that are under common control should be listed individually
- Product sales that included personal data transfer in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of a business to another company

227. Private companies should publish corporate statements on how they implement the UN Guiding Principles on Business and Human Rights, and integrate human rights due diligence throughout their supply chain and servicing, develop rigorous safeguards against abuse, human rights violations, and establish effective remedial mechanisms for children.

228. Families should be asked for opt-in consent before local authority or other linkage between nursery, primary, and secondary pupil data and commercial data broker records or other third-party data sources or data provided later in life such as from higher education, with exceptions, replacing routine linkage without consent and repurposing individual records.

229. Develop steps as part of Admission processes, annual updates, and on school entry/ departure to ensure families know that pupil personal data is collected by the school, for

Local Authority and to be sent to the national Department for Education or its programs, providers, research partners, governmental bodies, or regulators.

230. Children and families need to have meaningful routes to have their rights explained, or to exercise them and a way to be informed and seek redress when necessary throughout the educational lifetime. Enable mechanisms for communicating what edTech products will be used, for example, in the course of a year, on an annual basis and ensure ways of respecting all the rights afforded to families in making decisions about their use.

231. Ensure policy centres on the best interests of the child, which recognises that a person who has not yet achieved physical and psychological maturity needs more protection than others. Its purpose is to improve conditions for the child, and aims to strengthen the child's right to the development of their personality and character to the full. This protection falls to family, society, and the state.

232. Schools should continue to offer families the ability to make cash payments in schools when settings choose to switch to cashless payment systems for the purposes of all administration.

233. Recognise that ever greater permanency of data does not serve children well that need to learn from mistakes as they mature. Retention periods for third-party processors need to be reduced (often at 25 years) and given special attention because children merit additional protection. The default position for a child leaving school, should be that any personal data retained is held by the school as data controller, not the processor; and all pupil data held by third parties should be destroyed-by-default after transfer to the school.

234. Understanding how our personal data is used by others makes a difference to the balance of power in common interactions with companies and the state. Educational settings and providers have an important role in maintaining that balance if children are to remain in control of their own lives, with autonomy, able to make informed choices, see or object to discrimination, and understand interferences with democratic rights, as they grow up.

1.3.6.2 Findings 6 I Children's rights in a digital environment

235. In the rush to remote learning in response to the pandemic, children's rights have been ignored at speed and scale in 2020, more than ever before. We need to fix that to create a safe and trustworthy digital environment in education, fit for children's future.

236. Article 8 of the ECHR provides individuals, including children, with the necessary means to protect a private sphere in which they can develop their personality.[93]

237. In a world that talks about ever greater personalisation, we are in fact being treated less and less as an individual, but rather as a comparison, and ranked according to how we measure up against other profiles built up from historical data, and our comparative outcome or likelihood of paying back that loan, judged and determined according to their collective past behaviours.

238. *"Boyd and Crawford's (2012)[94] observation regarding big data is particularly relevant in the AI context: 'Many (people) are not aware of the multiplicity of agents and algorithms*

[93] Wachter, S. (2017) Privacy Primus Inter Pares: Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights http://dx.doi.org/10.2139/ssrn.2903514

[94] Boyd, D. and Crawford, K. (2012). Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. 15(5) Information, Communication, & Society 662–679

currently gathering and storing their data for future use.' (p.673). This leads to the third area of awareness - Students, parents and teachers should be made fully aware of AI data harvesting, storage and sharing arrangements with informed parental opt-in consent and student assent obtained. This is supported by the recommendations from the IEEE (2017)." (Southgate, 2019)

239. While there is often debate on the risks to AI product development in education from privacy and ethics, there must be much more time for understanding given to the risks to children whose classroom experience, interactions, scoring, learning pathways, development and how they are perceived by staff as a result is all shaped by the expansion of computer-driven decision making and big data analytics that turn the human development in all its complexity and uniqueness of individuals, into simplified dashboards for comparison of norms and outliers and can result in focussed intervention on a few picked by "the data", at the expense of others.

240. The United Nations Committee on the Rights of the Child, in its 2016 examination of the implementation of children's rights in the UK, called for the UK State Party to introduce "*a statutory obligation at national and devolved levels to systematically conduct a child rights impact assessment when developing laws and policies affecting children",* and to *"publish the results of such assessments and demonstrate how they have been taken into consideration in the proposed laws and policies".*[95]

241. Children in England should expect that their rights will be prioritised and enforced so that they can entrust their digital identity to third parties and can exercise their right to education, without finding it means accepting exploitation by default. This trust cannot be overstated in a time of growing socio-political and economic uncertainty, and technological advance and against the backdrop of the algorithmic exams fiasco of the summer of 2020.

242. Children have a right to their reputation. Their reputations are increasingly shaped by the growing quantities of information available about them online. This not only influences children's interpersonal relationships, but may also have an impact on their ability to access services and employment as they enter adulthood. (UNICEF, 2018)

243. Over three quarters of parents polled in 2018 said (79%) if offered the opportunity to view their child's named record in the National Pupil Database would choose to see it.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.[96]

244. Ease of access to freeware technology in practice has far outstripped school staff and parental knowledge of their data rights and responsibilities. We need to be able to empower young people in everyday digital interactions as they mature but also ensure they have a clean slate at age 18 of what commercial companies may pass around about them as school children.

245. In the 2017 report, *Growing Up Digital,* the Children's Commissioner wrote, "*we are failing in our fundamental responsibility as adults to give children the tools to be agents of their own lives.*"[97] Nowhere is it more obvious and reprehensible than in the course of their own education.

[95] Unicef UK (2017) Child Rights Impact Assessment https://www.unicef.org.uk/publications/unicef-uk-cria-2017/

[96] defenddigitalme (2018) Only half of parents think they have enough control of their child's digital footprint in school https://defenddigitalme.org/2018/03/only-half-of-parents-think-they-have-enough-control-of-their-childs-digital-footprint-in-school/

[97] 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

246. Children are disempowered by their age and capacity. Parents with concerns do not want to be seen as problem parents and rarely have the time or capacity to question data collections. Statutory collections mean that staff are habitualised in the belief that consent is not required which is conflated with not informing parents or telling them when data is ascribed by school administrators or Local Authorities.

247. Parents should be involved in the consent decisions of their children unless the competent child specifically objects, or there are reasons against it in the best interests of the child. Local authorities should establish a default position of involving parents in decisions about sharing their children's sensitive data unless a competent child refuses such involvement. (Dowty, 2009)

248. Most importantly children's own views are rarely taken into account. It is a myth that young people don't care about privacy. The 2017 edTech book edited by Rosemary Luckin, *Enhancing Learning and Teaching with Technology: what the Research says,* mentions privacy not from the adults advocating more data collection, or even in the opening chapter on the role of genetic inheritance in education, but in the section Pupil Recommendations, from the Year 7s, children aged 11-12, who said, *"increase privacy for pupils; stop spying on us."*[98]

249. Livingstone et al. (2019) documented how children care about their privacy online, that they want to be able to decide what information is shared and with whom, and further they found that, "*teachers are unclear what happens to children's' data and there is common misunderstanding of how much data leaves a school:*", "*The only time it does [to the government] is when we do the Year 11 data [...] Because obviously they'll do the tracking of different groups.*", (teacher, London) and when it comes to using educational platforms teachers assume some sort of quality control has already been done, "*I would've thought the fact that it's a school-based software, this has all been properly regulated.*" (teacher, London)

250. The Council of Europe 2016-21 Strategy on the Rights of the Child,[99] has an entire section on the digital world. It makes clear that, *"Children have the right to be heard and participate in decisions affecting them"* and recognises that capacity matters, *"in accordance with their age and maturity"*. In particular attention should be given to *"empowering children, such as children with disabilities."*

251. Lawmaking and procurement at all levels of government do not yet respect the UN General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights: "*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.*"[100]

252. The Difference report (IPPR, 2017) set out the economic impact of high levels of exclusions and the additional educational needs and high numbers of children with complex needs that are overrepresented in excluded children. The government should assess the economic impact expected by contrast if support was offered from the Early Years through an

[98] Luckin, R. (2017) ed. Enhancing Learning and Teaching with Technology: what the Research says, page 86 in the chapter 2.6 Learning with iPads Patricia Davies, Pupil Recommendations

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

[100] UN General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights (B(1)(27) https://www2.ohchr.org/english/bodies/crc/docs/GC/CRC-C-GC-16_en.doc

automatic award of an Education, Health and Care Plan upon application for children to uphold their right to education.

253. Families polled, want to be offered an opt in/out to school census pupil data third-party reuse especially for special educational needs and disabilities (SEND) data. 81% of parents agreed that parental consent should be required before a child's SEND data is shared with third-parties. Parents of children with SEND routinely need to wrangle a computer-says-no mentality to get their legal entitlements to education and care.

254. Families that find their child referred to the Prevent programme, have little remedy to correct false opinions or mistakes and the government failure to make sure the Independent Review was carried out as it should have been in law by August 31st 2020, lets down the vast majority of people wrongly referred[101] of whom an unknown volume may be as the result of their interactions with school imposed Internet Monitoring software in school or at home.

255. The UN Special Rapporteur's 2014 report on children's rights and freedom of expression stated: "*The result of vague and broad definitions of harmful information, for example in determining how to set Internet filters, can prevent children from gaining access to information that can support them to make informed choices, including honest, objective and age-appropriate information about issues such as sex education and drug use. This may exacerbate rather than diminish children's vulnerability to risk."*[102]

256. Developers may both intentionally and unintentionally shape how children are affected through their systems' design. There are no statutory boundaries of how far a third-party is permitted to nudge a child's behaviour, how they affect a child's mental health, how they profile and judge a child's performance, how they judge the intent behind a child's Internet search, and what data analytics they process. All these decisions are dependent on companies that are subject to change of control at no notice, through sales, mergers, private equity and takeovers. These decisions shape children's education and their lives.

257. While it may be convenient particularly where high street banks have closed down and processing cheques and cash has become increasingly difficult, using third party cashless payment providers should not be considered part of a public interest statutory requirement and offer no alternative. They are not consent based systems, when schools give parents no choice but to use them whether privately using their own device or through a PayPoint in a shop.

258. As ever more data is collected about individual children at a national level, we must ensure safeguards are in place so that unique lives are not misrepresented as simply outliers in a dataset that requires normalisation. Too many among the proliferation of products right now encourage flattening of outliers and conformity to standardisation. Even so-called personalised products, often simply find patterns in behaviour and compare it to that of other children, therefore standardising and norming the 'adaptive' offering once again not to you, but a child 'like' you and we have seen the harms this can cause, through the experience of thousands of children and young people affected by the 2020 exams awarding process.

[101] Grierson, J (2019) The Guardian | Family wins fight to delete child from Met's anti-radicalisation records https://www.theguardian.com/uk-news/2019/dec/19/family-wins-fight-to-delete-child-from-met-prevent-anti-radicalisation-records

[102] UN Special Rapporteur (2014) The right of the child to freedom of expression A/69/335 https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx

1.3.7.1 Recommendations Seven | Local authority and regional data processing

Children’s rights appear to have low priority when it comes to procurement or research projects. Many products influence behaviours, choices and habits and there is little transparency for families how these tools shape their child’s educational experience or what and how they learn. To restore a rights respecting relationship between families and schools when it comes to edTech, then the controller/processor boundaries need redrawn between edTech companies and educational settings and this needs oversight at a higher level than single school, for example by MAT or Local Authority.

For Local Authorities and equivalent MAT level service provisions

259. Only those Information Management Provider Systems must be procured that can enable schools and Local Authorities to manage granular data permissions with different controls on the same piece of data. i.e. ethnicity or Alternative Provision census data.

260. Public Authorities should document and publish a register of the datasets they are processing, to increase transparency of what educational data and personal data they process about children, including commercially obtained sources of personal data collected for processing, or linkage with data provided by individuals in the course of their public sector interactions. (i.e. Data brokers, companies, social media) Publish Data Protection Impact Assessments, Retention schedules, and any GDPR s36(4) Assessments with reviews to address changes.

261. Public Authorities should document and publish a register of the commercial processors / sub processors they engage in children’s data processing and which datasets each is involved with to increase transparency of who processes which data.

262. Government at national and regional levels should produce high level organisational charts of education services, and how the various organisations interact when it comes to roles and responsibilities, transfers of money and information. That gap today contributes to poor data management and lack of accountability and oversight for keeping families informed.

For educational settings and providers

263. Terms and conditions should be agreed with service providers at a higher level than individual school settings and also retain flexibility for schools to require contract changes. (ie in Scotland due diligence and procurement is overseen at Local Authority level). Schools must stay data controllers not only in written contracts but in practice. Processors must stop doing all they might like to as regards passing data onto third parties that schools didn’t ask for, or repurposing it for product development even where set out under school contracts. This happens today on a manufactured ‘consent' basis in UK schools, which fails children and parents. Companies need to offer stability in terms and conditions throughout the school year, with agreed notification process for necessary change, and reasonable terms. Families should get a consistent list each year (and at each school transfer) to explain the products their child will be expected to use— and crucially, legal guardians must be able to retain a right to object. Schools must be obliged to offer an equal level of learning provision via an alternative method, so that any objection is not to the detriment of the child.

264. Local Authority or national data processing must have a clear and workable chain of communication through schools to families. For example in the communication of Alternative Provision school census data transfers. Where nationality, country of birth, or passport data is retained for Tier 4 visa or other purposes in the School Information Management systems, it should be made clear when they are retained for local or national purposes, in particular where data is passed on to the Home Office, and for how long and why. These data should

be collected for this narrow and specific purpose and transparently processed to the pupil, family and/or their agent.

265. Companies contracted by schools have an obligation to inform the child/family how their data is used. This applies throughout the life cycle of the data processing, not only at the point of collection, and must be in clear and easy to understand language for a child, in line with data protection legislation. We would design a new framework for managing this through schools.

266. Reduce and simplify the number of policies given to parents on admissions. These often come as thirty separate, multi-page documents, and third-party commercial companies are commonly left out of explanations in privacy notices and retention schedules.

267. CCTV and other cameras should be made unlawful in toilets and bathrooms in all educational settings, and exceptional classroom use needs statutory guidelines and oversight from the Surveillance Camera Commissioner.

268. Non-essential biometric data processing should end where it is excessive and less invasive offerings are possible in line with other regulatory rulings after the introduction of the GDPR i.e. fingerprint readers for low security and routine transactions in canteens and libraries should be replaced with PIN and card systems.

1.3.7.2 Findings 7 I Local authority and regional data processing

Capability and capacity

269. Competence, consistency, confidence and capacity must improve across the education sector from Early Years through Higher Education when it comes to staff understanding of the digital environment, data management, and children's rights.

270. According to a survey carried out in 2018 by The Key,[103] schools were ill prepared to appoint Data Protection Officers, indicating a poor readiness despite pre-existing data protection law.

271. In a small and informal survey of school IT staff in the UK in March 2018 we commissioned: Over 75% disagreed that their school current data protection policies and practice met good data protection standards, or that they were confident and ready for the GDPR.
    - Over 65% of schools never inform the child or parents which personal data have been shared with an external third party when assigning new accounts with apps or technology platforms
    - Only 17% performed any regular data audit from the school's pupil information management system to have oversight and traceability of pupil data distribution. Their systems don't offer that functionality.
    - Almost a third indicate that their schools did not have data protection duties assigned to anyone at all three months before the enforcement date of GDPR and despite the fact that UK Data Protection law had been an obligation for over twenty years.

272. At the regional and local settings level, there are too few staff with limited knowledge and capacity to perform the necessary level of due diligence in procurement, with the required level of technical and functional capability to understand many of today's products and range of relevant law which go beyond the GDPR but require understanding of children's rights, human rights, equality, communications and privacy laws.

[103] Schools Week (2018) Half of schools aren't ready for GDPR https://schoolsweek.co.uk/half-of-schools-arent-ready-for-gdpr-data-protection-officer-requirement/ (accessed April 2, 2018)

273. Almost every human contributor to the education of a child today, is also involved in the creation, use or distribution of information about the children in their care. People that collaborate in any organisational unit -- a school, a governing body, a Multi-Academy Trust, a Research network, flow data within, across and outside that organisational unit. Each playing different roles -- their level of responsibility and accountability for decisions how the data is managed, shape their data duties, in data terms, as Data controllers and Data processors.

274. The House of Lords Select Committee on Artificial Intelligence report, *AI in the UK: ready, willing and able?* published in April 2018[104] recommended in particular, that the ethical design and use of technology becomes an integral part of the curriculum. That should be broadened into digital rights and understanding but it cannot happen until teacher training enables it.

275. Staff do not question why data is to be sent to the Department for Education and those who do, may often be met with well-intentioned but misinformed advice as was demonstrated in the 2016 school census expansion. They don't know what they don't know. In schools it results in distributing privacy notices that are misleading or not distributing information at all.

276. Thus a fairness fallacy ensues. Ever more data is created and collected in schools and lasts a lifetime in national records, but staff, parents and pupils have limited understanding of its use. This combination means that children and parents have no oversight or control of what data is collected, where they go, who has them, for how long or why.

Lack of transparency and information

277. A transparent organisational framework in which to understand a child's digital journey within the education system is missing. There is no easy way for a child or parent to understand the structure of the state education system, and therefore what flows of data exist between organisational units.

278. A child's learning journey is fragmented between multiple institutions supplemented by numerous companies without interoperability, multiple different usernames and log-ins and no single view of their shared view of pedagogy or learning goals. Maths alone in a school might be using a personalised learning platform, three different apps to quiz in the classroom and practice at home, as well as the school platform of choice. How many are necessary and proportionate? There is no one with joined up accountability for a child's digital footprint as it travels between institutions and their supporting third-parties across a child's education.

279. Knowledge from the child's data benefits primarily the company for product enhancement or development, but not the child as they transfer between year groups or settings.

Design functionality and lack of suitable tools for families and children

280. School Information Management Provider Systems tell us it would be too expensive for them to manage granular data permissions and this fails schools that then cannot meet their data processing obligations distinctly at local and national levels. For example, the family may be content for a school to know and retain information about nationality or adopted-from-care, but not want those same data to be sent to the Department for Education in the school census. Right now in most systems, nationality is either present in the system field, or it is refused. It cannot show that it is both at the same time. This results in the maximum rather

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

than the minimum data being collected at local level and all fields being sent, where held, to the Department for Education in a school census without any choice.

281. Despite the opportunities that digital transactions should be able to offer, there is often little value-add above and beyond a replacement for paper. For example, a school-home email or messaging service might not be offered in the parents' native language.

282. A meaningful framework and tools are missing for explaining the fair use of a child's digital footprint from the classroom for direct educational and administrative purposes at local level, including commercial acceptable use policies. What is required and what is optional in the termly school census? What goes to the government and what goes to companies? Model reports that give information annually to families accompanied by teacher training would deliver clarity, consistency, and confidence to school staff.

283. Digital understanding for all is required. But we cannot allow companies to use flawed notions of consent and ownership to push the onus for accountability back to our own actions alone. Having a digital understanding should not mean that an undue burden of understanding or obligations to point out problems in certain products or raise objections, is pushed back onto children and parents when they have no effective tools to exercise their rights in school settings. There must be a stronger partnership between schools and families and the consistent tools to allow communication of information rights and to exercise them.

284. Exam grade calculation is a black box of decision making based on historic data and comparable outcomes every year. The exam results fiasco of 2020 exposed an obvious gap in transparency and accountability: there was no at-a-glance report available that schools could use to explain to a candidate how their result was calculated using historical data, their own exam performance, and the standardisation process. That kind of tool is needed every year for schools to be able to show how their grades, or own data inputs combine with national comparable outcome calculations and result in overall grades for each pupil.

Lack of democratic engagement and public consultation

285. The volume of data transfers and stakeholders involved in education today is excessive and grows without families knowledge or ability to object to expansion.

286. Monitoring third-party intentions and appropriateness for schools impossible to manage in a meaningful way in the current lack of oversight framework. Unless we reduce the overall number of external actors, and poor quality products involved in the data processing of children's data in schools, and have properly and professionally assessed standards, bad practice can only be identified on a case by case basis but may affect hundreds or more schools simultaneously. For consistent, trustworthy standards an overarching quality model for product approval and oversight is needed before outsiders obtain approved access to school children's digital life.

287. The boundaries of what is ethical as well as lawful have become blurred using technology in schools and that can reach into children's private activities, space and time. In a trial of up to three years, ending in February 2013, pupils at West Cheshire College wore tags that allowed them to be tracked in detail throughout the college's three campuses. "*The technology was introduced with the aim of assessing how it could be used for self-marking class attendance registers, safeguarding purposes, and to improve the physical management of the buildings.*"[105]

[105] Grossman, W. (2013) The Guardian | Is UK college's RFID chip tracking of pupils an invasion of privacy? https://www.theguardian.com/technology/2013/nov/19/college-rfid-chip-tracking-pupils-invasion-privacy

288. It is increasingly common to see news reports of CCTV in school toilets[106] and parents upset at the intrusion and lack of consultation. There is no corresponding evidence of effective behaviour change as a result of introducing cameras in cloakrooms or all school surveillance and yet parents find themselves disempowered when decisions are made that they feel breach their children's rights. An ombudsman should be available to parents for appeals.

1.3.8.1 Recommendations Eight | Higher Education

The data industry that now operates in the Higher Education sector is vast and includes student surveillance 24/7, across campuses that increasingly strive to be smart, across the student whole experience from academic attainment and predictive analytics assessing 'risk factors' for drop out, to a lifetime of alumni fundraiser calls. Everyday data collections sit behind the infrastructure for building access and attendance registration and administration using fingerprint readers for the interface with printer and cashless payment systems. Universities surveil social media for reputational risk, online activity for the Prevent programme and the Student Loans Company may scan every social media for signs of fraud. Learning and attendance data are repurposed for tasks the data were never designed for in predictive analytics and even mental health risk indicators. Voice activated routine support services that process biometric data excessively, risk [107] trivialising high value biometric data. The young applicant on the cusp of adulthood remains deeply disempowered.

289. Applicant equality monitoring data at UCAS, HESA and higher education settings must be anonymised and aggregated at the point of collection and only statistics should be shared across different organisations including national funding bodies.

290. Data collected in the process of a student's administration and education should not be automatically assumed for repurposing in student data analytics or predictive data analytics programmes. This must be a separate process, operate on opt-in basis and with the possibility to withdraw consent at any time. The choice must be freely given and not have any detrimental effect on the student that chooses to withhold consent.

291. Settings should be obliged to publish registers on their institutional website in a proactive approach to transparency over their adoption of data surveillance services and systems, including third-party data analytics, predictive analytics, social media scanning, plagiarism detection, remote proctoring, and all third-party data processing purposes beyond the student years for the full data life-cycle of a student not only at the time of collection. Since a duty of fair processing already exists there should be no concern over risk to their institutional commercial or competitive interests. But this should not be hidden away across various privacy notices and instead offer a single-view to the student of all such data processing.

292. Applicants must be protected from historic Prevent programme referrals being passed on to Higher Education institutions without their knowledge, or having the opportunity to correct inaccurate data or object, ahead of the information transfer.

293. The Student Loans Company should increase their transparency and simplify their access to information that is for the benefit of students, such as about funding in particular for part-time learners and what the information requirements are at each stage rather than focus their efforts disproportionately on covert data practices for the purposes of fraud detection.

[106] Diebelius, G. (2018) Metro School ordered to remove CCTV after fitting cameras in toilets https://metro.co.uk/2018/07/05/school-ordered-remove-cctv-fitting-cameras-toilets-7685135/

[107] L.U. is a voice-enabled 'digital friend' answering current student's questions about things like their academic studies, timetabling and campus life through the iLancaster app and Amazon Echo devices at Lancaster University. https://www.lancaster.ac.uk/student-and-education-services/disability/prospective-students/lu-app/

294. The Student Loans Company should end their surveillance of students' social media. Investigations for fraud must not communicate to the institution until suspicions are proven fact and the student's well being is assured, in particular in the case of estranged students.

295. Monitoring social media by Higher Education institutions for the purposes of reputational risk should not include individual student social media accounts even where used in non-targeted ways because it means students are disproportionately likely to feature.

296. Remote proctoring should be a consensual process with a guaranteed right to an alternative exam invigilation process, and without detriment to the students that opt out.

297. Institutions should be obliged to publish statistics on their use of plagiarism detection systems. Students are treated by default as potential essay cheats by plagiarism detection algorithms. The psychological and stress consequences for students of being under constant forensic, automated surveillance, deserves more attention before systems' adoption.

1.3.8.2 Findings 8 I Higher Education

298. The majority of applicants (90%) in a UCAS survey of their 2015 UK applicants[108], agreed with the statement that they should be asked for consent before their personal data was processed for various purposes. Over twenty times more than disagreed (4%) with that statement. The majority of respondents were happy for their data to be shared for research purposes where there is a clear public benefit, and also on a consent basis.

299. A further 8% of applicants suggested that they would rather share no data at all with UCAS and not apply, than have it shared. In our own discussions with under 35s on the use of their data, it is often those who already feel most marginalised and stigmatised, including BAME and LGBTQ+ communities, who are in the group most likely to want to maintain control over their data and may be the very minority that 'inclusion data' seeks to understand but will exclude as a side effect of the way it is collected.

300. Equality Monitoring data from students in Higher Education are passed on from UCAS and universities to HESA, the Higher Education Statistics Agency Ltd. HESA passes these sensitive and personal confidential information on to other funding bodies. These sensitive data[109] now sit on a named basis in multiple national databases, including the National Pupil Database at the Department for Education, where it may be linked with hundreds of other pieces of personal confidential information about each individual, in their lifetime record starting from age 2. There is no justifiable necessity for distribution of named data in this way that is proportionate to the risks to fundamental rights and freedoms.[110]

301. Local Student Information Analytics at Higher Education institutions, may use student characteristics and behaviours in dashboards, business intelligence and key performance indicators. The types of data these analytics software range from[111] applicants and students' personal data from general registration, use of Virtual Learning Environment interactions,

[108] UCAS Applicant Data Survey (2015) 37,000 students responded https://www.ucas.com/corporate/news-and-key-documents/news/37000-students-respond-ucas%E2%80%99-applicant-data-survey

[109] HESA distributes sexual orientation, religion and disability data collected from students at individual, named level https://web.archive.org/web/20190726172535/https://www.hesa.ac.uk/collection/c18051/a/sexort

[110] The Department for Education (DfE) holds sexual orientation data on almost 3.2 million people, and religious belief data on 3.7 million people. The records go back to 2012/13, so include both current students and those who have finished university. https://defenddigitalme.org/2019/07/statement-on-student-religion-or-belief-and-sexual-orientation-data-in-the-national-pupil-database/

[111] Shacklock, X. (2016) From Bricks to Clicks Report https://defenddigitalme.com/wp-content/uploads/2018/12/frombrickstoclicks-hecreportforweb.pdf

processing financial data, alumni data, course data and interactions with facilities, such as libraries and e-books. It may also be used for analysis of workforce data held by the university.

302. *"The rise of education data science as an infrastructure for big data analytics in education",* wrote Ben Williamson in Big Data in Education (2017)[112]*, "raises significant issues about data privacy, protection and the responsible use of student data. In a recent news article it was reported that the company Blackboard had conducted a massive data mining exercise on student data from 70,000 courses hosted on its learning management platform."*

303. Jisc are seeking[113] to *'make the market'* for UK learning analytics, including working with Civitas Learning. But compared with the efforts for the institutions, there are few efforts to explain what the data mining means for students while institutions and vendors can benefit from "*economies of scale; better understanding of solution pricing; mitigation against lock-in; ability to benchmark against peers; general 'de-risking'; and for vendors: reduced cost of sales; and lower barriers to innovation."*

304. Northumbria University[114] provided 97 pages about their pilot use of learning analytics software from Civitas Learning International in 2017. That material did not include information about the use of algorithms because, *"Northumbria University does not hold a copy of any algorithms being used in this pilot."* They also withheld some information, applying an exemption because the University considers that the release of such information at this stage of the pilot could prejudice its own commercial interests. Students and applicants have a right to be informed when such automated decisions may affect them and currently they are not.

305. At the Student Loans Company, (SLC) Counter Fraud Teams have access to a number of social media sites including Facebook, Twitter, LinkedIn, Instagram and My Space. In January 2019 [115]however, there was no definitive published list available from the SLC of which platforms may be monitored, even though such sites are used as and when necessary as part of an investigation.

306. Organisations monitoring students' social media are currently on the rise but it still appears the exception that universities will monitor individual students for interventions. In 2017, the University of Buckingham began keeping tabs on students' social media posts to check whether they are showing signs of mental health problems, such as anxiety or depression.[116] However we are increasingly being made aware of anecdotal evidence of the chilling effect of academic institutions that ask teachers and academics to show restraint on social media in what they may state publicly, even on comments made in a personal capacity.

307. We did not research the widespread use of plagiarism software, its data processing or effects. However this topic needs assessment of the effects of its use on students and needs better research to see the application in UK universities through a UK lens and also respect cultural norms. Students are treated by default as potential essay cheats by plagiarism detection algorithms. The psychological and stress implications of being under constant surveillance deserves more attention. Contract cheating services and getting others to write your work in 'essay mills' are not new, but the speed and scale of services thanks to online

[112]Williamson, B. (2017) Big Data in Education: The digital future of learning, policy and practice. London: SAGE. https://us.sagepub.com/en-us/nam/big-data-in-education/book249086

[113] JISC, Creating a collaborative, integrated learning analytics service (2016) https://web.archive.org/web/20200730141412/https://www.jisc.ac.uk/blog/creating-a-collaborative-integrated-learning-analytics-service-fit-for-the-sector-25-jul-2016

[114] FOI request whatdotheyknow.com Northumbria University https://www.whatdotheyknow.com/request/442550/response/1078833/attach/2/20171201ResRFI1905.pdf

[115] FOI request via whatdotheyknow SLC Student data sharing: policies https://www.whatdotheyknow.com/request/student_data_sharing_policies

[116] Gray, J. (2017) Huffington Post | University Of Buckingham To Monitor Students' Social Media Accounts To Tackle Depression And Suicide https://www.huffingtonpost.co.uk/entry/university-of-buckingham-students-social-media-accounts-depression-suicide_uk_588b5196e4b02f223a01a178

access has changed universities' approach to dealing with them and investing in services to combat rather than solve the issues. A diverse student population will inevitably reflect different approaches to research and reference to others' work may and written work without appropriate credit, may not be intentionally submitted to be fraudulent, signal guilt or lack of integrity. What automated systems may pick up as plagiarism may also reflect poor referencing, diverse approaches to learning, a respect for the authority of others' work particularly where this is a cultural expectation in early stage university students, unfamiliarity with the expected boundaries of collaboration versus 'cheating' by sharing work, or limited writing experience or experience in the use of English as an additional language. (TES, 2020)

308. Online proctoring can have significant harmful outcomes on human dignity regardless of technical functionality because of how it changes candidates' experience and how it makes them feel. Even privacy preserving solutions may negatively affect students' human rights.

309. Automated surveillance and automated decisions without adequate protections for human rights, safeguards from harm or that offer accessible and meaningful routes of redress can have lifelong consequences for young people. Whether lessons have yet been learned from the TOEIC [117] experience by the UK government appears doubtful in the aftermath of the exams 2020 fiasco.[118]

310. There are a number of disasters waiting to happen at scale, either as a result of accident or abuse in Higher Education. The question is perhaps only whether the misuse of named equality monitoring data, the loss of a mega database of anything a student has ever done and written from third party plagiarism or learning analytics platform, or a compromise of student biometric voice data, will be the first to grab the news headlines.

1.3.9.1 Recommendations Nine I Research

There is no single definition of research, or reference point for the volume and location of trials, testbeds and industry-led projects going on in schools in England. What the application of these various testbeds, projects and trials can mean for a single child across their educational life is not clear. Organisations carrying out research trials and not subject to Freedom of Information decline requests for transparency statistics. It is impossible for us to research this at school level due capacity and it would be costly for schools to ask at scale, how many trials are typically going on at any one time across the sector. But it appears a glaring gap in understanding how much and which children are subjected to what kinds of interventions in their classroom or school-led activity at home. No single organisation appears to have oversight or be accountable for these activities

311. An independent oversight board should be established for every product and research trial application in educational settings and published in a review and approvals' process, Its structure along a similar model to the Confidentiality Advisory Group (CAG) in health.

312. The board and independent ethics oversight process should be established within the remit of a new national data guardian for education with audit access to all trials in educational settings or involving children and a high standard of ethics should be applied, as in health.

313. A single national view should be publicly available of the volume of research, third-party access to schools, their intentions and outcomes. Every product trial and research intervention in educational settings must be registered in an open, free-to-access, national transparency register.

[117] Bulman, M. (2019) Home Office revoked tens of thousands of visas using 'misleading, incomplete and unsafe' evidence, official report reveals https://www.independent.co.uk/news/uk/home-news/home-office-english-tests-foreign-students-toeic-scandal-evidence-appg-report-a9008211.html

[118] Wright, R. (Financial Times) 2019 How thousands of foreign students were failed by the Home Office: A scandal over an English exam raises fundamental questions over UK immigration policy https://www.ft.com/content/11663990-1924-11e9-b93e-f4351a53f1c3

314. Every Privacy policy, Data Protection Impact Assessment, Legitimate Interests Balancing Test, and Research Ethics paperwork should be published and linked to within that register.

315. The register should be easily searchable by setting name, and by postcode, transparently publishing which trials are live and which schools have participated in, in the past.

316. The public benefit must be a prerequisite for research ethics approval for trials in state schools and other educational settings and findings published after completion of the trial.

317. Trials with interventions in live classrooms that take time away from the child's regular school activity and designed for trial purposes must be made opt-in by consent only.

318. Parents and children should be offered a Right to Object to data distribution in product trials or research projects regardless of the legal basis for data processing.

319. Children's routine state education time should not be used to generate private for-profit products from product trials in particular when children have no choice but to attend.

320. Behavioural science, neuroscience, personalisation using real-time or historic profiles, facial recognition and gait analysis, nudge, affective tech, immersive VR, and other emerging technologies should not be routinely trialled in state education because the effects may be significant and lasting but currently may be poorly understood. Any controlled research studies should require independent ethical oversight, registration, and opt-in consent.

321. Routine administrative tools that schools ask families to use for tracking sickness and absence should be opt-in not opt-out for all indirect reuses including research purposes.

322. The Behavioural Insights Unit, The Education Endowment Fund, Institute for Effective Education, Nesta, The NFER and The Sutton Trust and other similar organisers of trials at scale involving children, should immediately publish a list of all their current and past trials involving UK school children. Information should include how many children are or were involved in how many schools, including the implications for children at settings designated as Associate Research Schools and the nature of trials, whether on an interventions or data-only basis and the nature of the intended outcomes.

323. Police for the purposes of criminal investigation, and the DWP for purposes of fraud investigation, have begun to get access to the National Pupil Database at pupil level for interventions. This increasingly jeopardises the public trustworthiness of all public interest research. The same data can no longer be maintained indefinitely at pupil level for academic research purposes as its indefinite retention jeopardises children's fundamental rights and freedoms being held at national level. The linkage of administrative datasets at national level remains without a social contract and there appears to be no appetite at the ADR to resolve this. Therefore the organisations are failing to meet their DPA obligations for researchers and access should end.[119]

1.3.9.2 Findings 9 I Research

324. The definition of scientific research purposes has substantial ramifications for the range of data processing activities a controller may undertake. The term 'scientific research' is not defined in the GDPR. Recital 159 states "(…) For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner. (…)", however the EDPB considers the notion may not be stretched beyond its common meaning and understands that 'scientific research' in this context means a research project set up in accordance with relevant sector related methodological and ethical

[119] ADRN (2016) ADRN guidance for researchers http://www.adrn.ac.uk/media/1202/section_33_dpa.pdf 06/03/2016

standards, in conformity with good practice.[120] Recital 33 does not disapply the obligations with regard to the requirement of specific consent.(EDPB Guidelines, 2020)

325. A number of initiatives financially incentivise schools to provide their pupil's data for research purposes and there is no oversight how often this happens or mechanisms for parents to understand it. This means that there is no oversight how disruptive such interventions may be to a child's learning or well being across their educational experience as a whole.

326. There are significant implications for children from human rights and ethical perspectives.

327. Researchers may see personal data from children, students and staff published on social media as "fair game"[121] when in fact using personal data needs to respect human rights under data protection law by both academic researchers[122] and commercial developers. They must meet their obligations and not only pass duties back to their data sources and schools without any accountability for whether necessary processes such as fair processing happen.

328. In other work, small academic trials can be going on in schools at any time in regular lessons. Large scale trials involving thousands of children at hundreds of schools, can take place as part of regular school activities. Parents are not always asked for consent and may be refused requests to withdraw children from interventions because they are set up as part of regular, whole-class activities.

329. The Research Schools Network is a collaboration between the EEF and the Institute for Effective Education (IEE) to fund a network of schools which support the use of evidence to improve teaching practice. Launched in 2016, the Network currently numbers 37 schools: 27 Research Schools and 10 Associate Research Schools. All have been appointed following a competitive application process. Applicants need to have the capacity and reach to connect with up to 200 schools in their respective regions. The Research Schools Network aims to lead the way in the use of evidence-based teaching, building affiliations with large numbers of schools in their region, and supporting the use of evidence at scale. (EEF, 2020)[123] Highfield Nursery school Ipswich, was the first early years setting to join the Research Schools network.

330. The Nesta EdTech Innovation Testbed in conjunction with the Department for Education to trial 'software, such as apps, websites or online programmes' launched in mid 2019 and explicitly tells participating schools on its website that there is no need for individual consent. In doing so they appear to conflate a lawful basis for researchers' access to the data with the third-party processing. The only lawful basis for processing mentioned, is vaguely public interest, which does not take into account the processing by the product company, or the potential additional legal requirements when processing children's special category (sensitive) data. *"Since this project is generating evidence on products to help existing school and college objectives, and is in the public interest, there is no need for individual consent."*[124]

331. The boundaries of the definition of 'research' goes beyond public interest statistical analysis and it is today used to cover a wide range of interventions with children in their everyday

[120] EDPB Guidelines 05/2020 on consent under Regulation 2016/679 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[121] Hibbin, R.A., Samuel, G., Derrick, G.E. (2018) From "a Fair Game" to "a Form of Covert Research": Research Ethics Committee Members' differing Notions of Consent and Potential Risk to Participants Within Social Media Research, accessed March 25, 2018 http://journals.sagepub.com/doi/10.1177/1556264617751510

[122] Yildiz, D.,Munson, J. Vitali,A. Tinati, R. Holland, J (2017) Using Twitter data for demographic research https://www.demographic-research.org/volumes/vol37/46/

[123] EEF (2020) Research Schools https://educationendowmentfoundation.org.uk/eef-support-for-schools/#research-schools

[124] EdTech Innovation Testbed: FAQs for schools and colleges https://www.nesta.org.uk/project/edtech-innovation-testbed/frequently-asked-questions/

school activities. Children's personal data and findings from 'research' projects are being used in the development of commercial products. As Nesta explained about one example project in 2015,[125] *"Based on this work with teachers and students, Ai-Media UK has 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."*

332. Some products are simply piggy-backing research purposes on top of a school administrative app, such as for sickness and absence tracking that parents are asked to use across the whole school and while nominally use may be on a 'consent' basis it is hard to decline use.

333. While some third-party companies may offer an opt-out process for research reuse of school administrative data,[126] repurposing absence reporting and children's health data for other things with only an opt-out, for example, rather than active and freely given opt-in is poor practice for data relating to health under Article 9 of the GDPR. Inclusion in research data sets and processing special category data for "anonymisation" to create open datasets should require an opt-in consent, not rely on an opt-out or legitimate interests.

334. Companies that process children's personal data collected during the use of an app or platform routinely misunderstand the nature of the legal requirements of anonymisation for research purposes assuming their own repurposing of data for both product development by themselves, and by others, and passing on data for research purposes in pseudonymous or anonymised formats. They fail to grasp that as data processors they do not have the authority to make decisions about the nature and purpose of processing, that the act of anonymisation is of itself processing which requires its own legal basis for the processing and that such basis is generally absent. This leads to research without an adequate lawful basis or fair processing having been carried out with appropriate levels of accountability. (See case studies in Part 3)

1.3.10.1 Recommendations Ten I Enforcement

Good data management today in the sector is inconsistent and limited. To move forwards children need adults to fix what is currently broken and be accountable to children enabling them to understand and exercise their rights, rather than ignore them as usual today. It must be clarified quickly whether or not the ICO Age Appropriate Code of Practice applies to educational settings.[127]

335. Children need a strong approach when it comes to the protection and interpretation of their 'data subject's rights and freedoms' and 'significant effect' because they are still developing physically and mentally and their own and families authority in schools is disempowered.

336. UK regulatory enforcement (of data processing that does not meet legal requirements aligned with the GDPR, the Data Protection Act 2018 or Convention 108 and PECR) should be carried out consistent with GDPR regulatory action to date in the education sector; such as in France, Sweden, Norway, and Poland. A UK sector wide-review of certain areas of pupil data processing, rather than individual educational settings may find many of the similar issues at national level pupil data handling, at local levels: lack of accountability, lack of fair processing or explanation of rights, over reliance on the public task and lack of lawful basis. Such a review might follow the lead of the Victorian Information Commissioner who

[125] Making learning visible: First 'Technology in Education' evaluation published. The results of our Visible Classroom pilot: source https://www.nesta.org.uk/blog/making-learning-visible-first-technology-in-education-evaluation-published/ (archived at https://web.archive.org/web/20190723002723/https://www.nesta.org.uk/blog/making-learning-visible-first-technology-in-education-evaluation-published/)

[126] Inspire (research on asthma in children) https://web.archive.org/web/20190222190434/https://everychildisdifferent.org/inspire

[127] defenddigitalme (2020) The ICO Age Appropriate Design Code and schools https://defenddigitalme.org/2020/09/the-ico-age-appropriate-design-code-and-schools/

published a report on an examination of the use of digital learning tools in primary schools, and how privacy issues are managed when these tools are selected and used.[128] They found, "*schools are at risk of breaching the information privacy principles when using apps and web-based learning tools that handle student personal information*." (August 2020)

337. The standard of sector-wide information and professional training on the GDPR has generally been of poor quality and often misleading on controller and processor roles, obligations and children's consent. There is a lack of in-depth experience in the GDPR training offerings often provided for by previous 'cyber-security' or IT specialists but not from qualified professionals in law and in privacy, communications, child rights and data legislation. Accountability for quality standards should be raised through intervention by the ICO in particular when gross findings at a school were not identified by third-party commercial GDPR trainers, and through certification and training.

338. edTech companies and research organisations that operate across the sector should be of priority for ICO enforcement. Lack of enforcement in the education sector has led to data protection being seen as a low priority in school settings.[129] But children's rights and responsibilities by design and by default will not be realised through single school improvement alone but rather by raising standards across multiple settings and dissuasive of poor practice at scale.

339. Basic principles of data protection and enforcement must be realised sector-wide. Obligations that apply to the necessity and proportionality of a task, the amount of personal data collected, the extent of the processing, the retention period of identifiable data are often least well understood and simply accepted by schools in 'click-wrap agreements' that they cannot adjust. In particular, such measures shall ensure that by default personal data is not made accessible without the individual's intervention to an indefinite number of natural persons is rarely considered as part of data protection by default and design.

340. The right to obtain human intervention on the part of the controller in automated decision-making must be offered proactively to families since children cannot exercise this right themselves.

341. An ICO code of practice should set out what is considered 'necessary and proportionate'. Not only in terms of the data processing within an app or platform, but whether that tool is of itself safe, ethical and necessary or whether a less invasive method of that teaching or learning or administrative exercise would be as necessary and proportionate to the task.

342. Data Protection Impact Assessments (DPIA) should be considered "high risk" when the risk is cumulative at scale across a range of settings by the same controller or processor.

343. Children need adults to rethink what is seen as a 'significant effect' for a child, which could be very different for a child than an adult, and address this appropriately in enforcement.

344. Obligations should be made on controllers and processors of biometric and body data to have a duty to explicitly register processing such data with the ICO where it concerns a child.

345. As many manufacturers are based abroad, or export abroad, enforcement collaboration is going to be important. Cooperation and consistency in particular as regards children's data with third countries, must take into account the countries' own regulations and mechanisms,

[128] Victorian Information Commissioner (Australia) examination into the use of digital learning tools schoolshttps://ovic.vic.gov.au/wp-content/uploads/2020/08/Examination-into-the-use-of-digital-learning-tools-in-Victorian-government-primary-schools-August-2020.pdf

[129] The Key (2020) Remote learning: considering the GDPR| Data protection won't be your number one concern right now https://schoolleaders.thekeysupport.com/covid-19/deliver-remote-learning/lead-your-approach/online-learning-considering-gdpr/

which could be outside the EU remit of the GDPR, however that serve well alongside the GDPR rights and enforcement. Cooperation on the basis of other mechanisms may be more effective than the GDPR alone, for example the Convention 108+ including the Additional 26 protocol to Convention 108[130] regarding supervisory authorities and transborder data flows (ETS No.181) and further Guidelines for Data Protection for Children in Education (forthcoming 2020).

1.3.10.2 Findings 10 I Enforcement

346. Data Protection Officer duties are often duties added onto staff with existing roles, such as Business Manager, and it is unreasonable to expect them to meet the key requirements of the GDPR Article 37(5) without specialist training and adequate time to give to the role. Shared services may be a better use of school resources and skills to have a dedicated DPO between schools who has the necessary legal expertise and data protection knowledge needed for the role as DPO, but even then the knowledge of edTech can be missing and needs strengthened to understand emerging technologies and the emerging harms.

347. Conducting a DPIA is a legal requirement for any type of processing, including certain specified types of processing that are likely to result in a high risk to the rights and freedoms of individuals. However data controllers may not be aware that their setting is only one of many that the same joint-controller or processor is processing for, so that a school class of thirty pupils may not be considered high risk and a school may not carry out a DPIA. But when no school does, and the same business manages the data for thousands of schools, it can be the case that no one has performed a DPIA because it is the duty of the controller. This can result in the cumulative high risk processing being underestimated.

348. The standard of sector-wide information and professional training on the GDPR has been of mixed quality, often misleading those receiving training in particular on controller and processor roles, children's consent and misstating obligations on schools when a child turns 13. Unqualified and unregulated training providers are able to misinform large audiences such as at trade shows and large scale events without redress. Certification should be required and demand high standards of legal knowledge as well as data protection practice, recognising that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

349. There is a failure to grasp and pass on critical legal understanding that the GDPR and data protection law is not all that matters when processing children's data. Privacy law, protection of communications, equality law, other child rights and international guidelines, safety and even employment law and court rulings may need to be understood and respected.

350. There has been little enforcement action reported to date in the education sector. *"In the second quarter of 2016, 40 data security incidents were reported to the ICO regarding the education sector, compared with 278 for the health sector, where notification is already compulsory. This means that incidents have been low, statistically speaking, so the action taken has been light and in the form of a managed "undertaking", whereby the ICO stipulates preventative and corrective actions that have to be taken within a set time frame. Since 2015, only two educational establishments have had to sign up to an ICO undertaking."*[131]

351. Without enforcement it is unlikely that we will see improvement on current practice in England. Without knowing the expected standards for ensuring that, by default, only

[130] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) https://www.coe.int/en/web/data-protection/convention108-and-protocol

[131] Oladuti,T. (2018) TES https://www.tes.com/news/school-news/tes-magazine/your-school-ready-gdpr

personal data which are necessary and proportionate for each specific purpose of the processing, and where less invasive methods are not available, data collection will continue to be excessive.

352. Avoiding security threats should become a stronger preventative action among enforcement action. The inherent risks of outdated systems include exposure to ransomware and other security threats[132] across the range of the education sector from primary school to Higher Education. Many of the universities that reportedly responded to FOI requests this summer, and confirmed they had had a ransomware attack, reported they dealt with multiple attacks, with Sheffield Hallam University reporting the highest number, 42 in the past seven years."[133]

353. Data minimisation must be prioritised. Few schools seem to do as good a job as John Taylor Multi Academy Trust (JTMAT) in Staffordshire, explaining all its third party processing on one webpage.[134] But each school could ask itself whether over 85 unique third-party processors of data routinely *necessary* for educating a child in state school? That is before adding the hundreds of DfE external data users of their national pupil record, further access for regional and local authority purposes and sub-contractors.

354. In 2018 Members of the House of Lords said in debate,[135] *"Schools routinely use commercial apps for things such as recording behaviour, profiling children, cashless payments, reporting and so on. I am an advocate of the uses of these technologies. Many have seamless integration with the school management information systems that thereby expose children's personal data to third parties based on digital contracts. Schools desperately need advice on GDPR compliance to allow them to comply with this Bill when it becomes law."* They championed children's agency, *"young people probably need more protection than at any other time in our recent history. They should have control over their own data."*[136] And they called for, *"Both children and parents [need] to be properly informed of these rights and the use to which data is put at every stage throughout a child's school life and, where applicable, beyond."*[137] Enforcement should ensure compliance, that rights are realised, and fair processing is meaningful not a 'get out of jail free card' simply by having a privacy policy posted on a website. Many parents will not know which companies process their child's data and cannot know where to begin to look for a policy, and some products are brand names that appear small, but on deeper research reveal a multinational conglomerate.

355. Schools are disempowered by standard contracts that companies will not edit. Excessive processing in UK schools has become normalised and does not have a lawful basis because the necessity in the performance of a public task has been so loosely interpreted both in schools, and commonly by their third-party processors. Companies will regularly claim to be processors when their actions demonstrate they are (joint) data controllers yet they fail to demonstrate any accountability for the responsibilities this requires including transparency of processing to the children, and responsibilities to meet Subject Access Requests.

[132] School districts are a particularly easy target for ransomware operators because of their low budget for information technology and limited security resources (2019) ArsTechnica https://arstechnica.com/information-technology/2019/08/rash-of-ransomware-continues-with-13-new-victims-most-of-them-schools/

[133] Ilascu, I. (2020) Over 25% of all UK universities were attacked by ransomware https://www.bleepingcomputer.com/news/security/over-25-percent-of-all-uk-universities-were-attacked-by-ransomware/

[134] Who do we share data with? John Taylor Multi Academy Trust (January 2020) https://jtmat.co.uk/privacy/who-do-we-share-data-with/ archived https://web.archive.org/web/20200911170527/https://jtmat.co.uk/privacy/who-do-we-share-data-with/

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

[136] Ibid, Lord Storey https://goo.gl/dKaJvX

[137] Hansard, col 1436 December 11, 2017 The Earl of Clancarty, https://goo.gl/FbBvxk

1.4 Definition of a child and education data

1.4.1 Who do we mean by a child?

In England broadly in education law as well as data protection law, a child is anyone aged under 18 except where stipulated otherwise. Although you can leave school on the last Friday in June if you turn 16 by the end of the summer holidays, you must then do one of the following until age 18[138]:

- stay in full-time education, for example at a college
- start an apprenticeship or traineeship
- spend 20 hours or more a week working, volunteering, in part-time education or training

This has implications for what data is collected from education data collections such as the censuses, and for how long. School statutory data reporting requirements therefore apply to everyone up to age 18. Some aspects of children's social care and education may also make statutory obligations for young people up to the age of 21 or 25, such as leaving social care or those with special educational needs and disability.

As regards data protection law, children are only aged up to 18 and therefore there are a number of years for young people who may be regarded as having additional vulnerability or in need of extra adult care, for whom their data rights are out of sync with their educational rights and data collection is inconsistent.

Compulsory education ages and definition of "pupil" are different across the UK, and within the meaning of the 1996 Education Act; the Education (Scotland) Act 1980, The Education and Libraries (Northern Ireland) Order 1986, or young people with special educational needs or disability within the Children and Families Act 2014.

In all cases, the best interest of the child carries weight, so data controllers are required to make it clear to children and/or their legal guardians what their rights are at the outset of any data processing, in a way that is meaningful and appropriate for the individual's circumstances.

Our research has shown that the complexity of roles and responsibilities means very often no one explains their data rights to a child or their family, or provides any way for them to be realised. This is acute when the data processing is done by a different agent than where a child physically attends, for example in the Alternative Provision Census where no LA had made that effort in 2018.

1.4.2 What do we mean by data?

It is difficult to imagine just how much information is created and collected about children throughout their education, or how that information is used, stored, and shared with others. Most data used in schools is ascribed by staff. While it may be fact based it can also be:

- **observed**, by tracking people with assessment comments online or on devices;
- **derived** from combining information with other data sets; or
- **inferred** from human opinion, or even machine based algorithms to analyse a variety of data, such as third-party sources via social media, location data and records of activities in order to profile people for example in terms of their behaviour, state of well being or safeguarding.

Core educational records were once the only data that schools would exchange as children move across the sector throughout their education.

[138] School leaving age across the UK https://www.gov.uk/know-when-you-can-leave-school

Now a child and parent may both contribute data to a multitude of software systems maintained by third party suppliers. School staff ascribe an often detailed set of opinions and adjectives that last a lifetime. Increasingly machine-assessed measures of behavioural profiling through points or keywords are used to measure and predict success or failure and databases store that prediction on a permanent record at local and national level.

Personal data from parents and the wider classroom or community can be part of a child's school record. Families are encouraged to comment on a child's profile from the Early Years Foundation Stage. At primary school, parents, carers and staff can comment on a child's digital portfolio. This may be stored on a cloud-based platform, with comments and photos of school work and the child.

Personal data is first collected by a school for the purposes of administering a child's admission to a school from legal guardians' applications to the state school system for a place. Once the place has been assigned through the Local Authority, more information is collected by a school directly from the legal guardians. Schools store this personal data in their management information system (MIS) — though the brand name acronym for the most commonly used system among 15 common UK providers, Capita SIMS[139], which supplies over 80% of England's schools, has taken on a common use.

Having started school, a child's individual named pupil record is managed and built up over the course of a child's time spent at that school through the MIS. Most systems are cloud based, and the data is therefore stored off site, with support from the provider companies. When a child moves between schools, the core of that record is transferred by the sending to the new receiving school, in what is known as the Common Transfer File (the CTF).

Schools manage their internal administration by accessing the core data held on the MIS through their chosen software and tools, for timetabling and planning for example. Schools then start to input their own data to a child's named record. This is added by school staff in the classroom and through administration. This can include behavioural records, or individual needs such as health and special educational and disabilities, safeguarding data that may come from or go to children's services, whether a child is entitled to free school meals and if the school can claim pupil premium (additional funding on a named-child basis, most commonly as the result of a child's family low income status).

All these types of data use and reuse are generally for the administration of a child's education and direct care from a school, while in loco parentis but those boundaries of school responsibility and reach into private and family life have become blurred as cloud-based processing allows surveillance and data processing 24/7, 365 days a year. Data collected by a school may now be from the child's homework, or all online activity at home.

The administration of the school can also involve outsourcing to private companies, that provide the capability to supplement on-site administration through technology so that the data is processed by and controlled by the company. For example, cashless catering systems are now common in UK schools to enable families to manage the pre-payment of lunch money, as well as payment for materials in food tech, art or DT lessons, or optional school trips.

Personal data created about and through a child's experience of learning are limited within the MIS. However, the number of actors involved in creating personal data about a child's learning outside of the educational record can be vast, where a school supplements teaching, classroom and homework activities, with digital tools.

[139] Johnson, C (199) TES Taxpayers lose in sale of software https://www.tes.com/news/taxpayers-lose-sale-software SIMS was born when a teacher at Lea Manor high school in Luton, wrote a program allowing teachers to produce computerised pupil reports. Bedfordshire county council then developed the scheme using thousands of pounds of its own money. By 1984 it was running a seven-school pilot project and by July 1986, every upper and high school in the county was using the system.

This raises questions over what is and is not part of a child's state educational record, who has control of that. Where data is held by third-parties can schools meet all their lawful obligations? For instance, if a parent asks for a copy of the educational record, it must be available within 15 days under the Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437). This is shorter than the month of a Subject Access Request and some companies may fail to provide information about a pupil in this time period and will only fulfil a SAR via the school as a go-between and decline to answer questions directly, even once a parental identity established by the school. This 4-way relationship child-parent-school-company is cumbersome in understanding a child record and while schools should rightly play a role in confirming a legitimate SAR request, companies that are data controllers should meet requests and answer questions directly, once the approved status is given.

1.4.3 Can parents consent on behalf of a child?

The 2009 report by Dowty and Korff addressed the law and children's consent to personal data sharing, and still holds true today.

> *It has long been the case that agencies can share information without consent about children whom they believe to be at risk of significant harm from neglect or abuse. It is also true that practitioners have always maintained case notes and discussed particular concerns with each other. However, what is relatively new is the question of whether children can consent to having sensitive data that they reveal to one person stored on a database and shared with others. In this instance, 'sensitive' means information about their mental or physical health, their beliefs and their private lives.*
>
> *Legal guardians act on behalf of a child and where children have competency, children can act in their own best interests. Children can also exercise rights over their data to the extent of forbidding others — including their parents — from having access to their confidential records.*
>
> *Government policy and children's online activities raise all kinds of questions about confidentiality and the integrity of data, and they push the vital issue of who can or should consent to the collection, storage and sharing of children's confidential information to the top of the agenda.* (Dowty and Korff, 2009)

It is common bad practice in schools to collect flawed 'consent' forms on admission, which are required acknowledgements rather than a valid consent process for data processing i.e. 'Please consent here.' We have not seen data collection forms that discern between local and national purposes. These forms need improvement for school admissions and school census processing to inform families what is collected for which purposes, ask for consent for optional items, and separate national from local needs.

Consent is often invalid. If a school or companies do ask for consent as their lawful data processing basis it can only be valid where a pupil or family has an informed and freely given choice, without bundled purposes, no pressure to agree, and no detriment to refusing. For example if a parent/child declines to use a consent-based AI platform that the school demands is used in the classroom, the school must be able to offer an equal educational alternative.

It is not valid to ask for consent to use a routine digital product in the classroom where children and parents cannot freely decline without detriment and such processing must be careful to address the reasons why the terms and conditions require consent. Often it is because the company is processing pupil data beyond the school remit. I.e. for the company's own purposes that it has chosen to carry out, not at the request of the school: product development, research purposes or passing data on to third parties. The Information Commissioner's Office guidance makes it clear public authorities, which includes educational settings, will have difficulty relying on a consent basis for data processing, given the power imbalance.[140] This is especially true for children.

[140] Article 29 Working Party guidance on consent http://defenddigitalme.com/wp-content/uploads/2018/04/wp29_consent-12-12-17.pdf

Consent will rarely be a lawful basis for processing data in a school. However for biometric data processing where offering an alternative is obligatory, freely given consent is required and schools must not process biometric data from a child if either a parent or the child objects. These protections are offered in England and Wales, under the Protection of Freedoms Act 2012. This legal obligation is often ignored (38% of families we polled where school biometric systems were in use in 2018, said they had not been offered a choice).

The idea that a 'digital age of consent' of thirteen applies to schools for all data processing is mistaken, or even that it applies to all the apps and platforms that schools require children use. Organisations that ask this of schools, appear not to understand data protection law, specifically the requirements of the GDPR, or the legal basis for pupil data processing.

The Department for Education data protection toolkit for schools (2018)[141] sweepingly states that "Parental consent will always expire when the child reaches the age at which they can consent for themselves (13 years old)." This adds to misunderstanding in some schools if, how and when consent is a lawful basis for processing children's data, whether 'information society services' applies to education apps data processing[142], and fails to address questions of capacity versus age, or the power imbalance that often invalidates consent.

Consent is sometimes asked for, where processing is excessive. Such processes also often make third parties data controllers, not processors, from a data protection perspective in law, although they will argue that "we are data processors as set out in our contract and terms and conditions." If so, then a processor should be doing nothing more than very narrowly that processing which a school has expressly required of them. But third parties often go beyond this, and determine the nature and purpose of processing. Extensive adTech analytics, third party re-use or repurposing for research distribution, or keeping data forever for their own product development even where de-identified, makes processing that relies on the school's public task likely unlawful and more likely that third-parties are [joint] data controllers.

In "Cookies That Give You Away: Evaluating the Surveillance Implications of Web Tracking," released in 2014, Reisman et al. explained how web pages with embedded trackers can connect a user's web page visits back to the specific user. Cookie consent is rarely valid.

Consent is rarely informed. Like the Department for Education when it comes to national processing, suppliers often fail to properly pass on necessary information to schools to allow the fair processing responsibility to be met, such as adTech third party processor re-uses, repurposing for research distribution, or keeping data forever for their own product development. Companies fail to tell schools which child's information was used for which third party purposes. Schools are therefore unable to meet this obligation that the companies delegate, and the companies in turn fail to meet their own accountability obligations.

It is impossible for a school to really understand how many of these digital tools work or see that data processing goes beyond what the school requires due to complexity and vague terms of service. Researchers at the Oxford University Department of Computer Science, revealed the extent of hidden ad trackers, in an assessment of nearly one million apps (Binns, Zhao 2018). If even the developers might not understand the full extent of what their code does when it comes to re-using third party data analytics and cookies for example, (Ekambaranathan, Zhao and Van Kleek 2020)[143] then suppliers cannot explain it to schools, and schools cannot to families or children.

In the same way that third-party data processing at national level from the Department for Education assumes fair processing is done, it falls through an accountability gap in local data processing too.

[141] DfE Data protection: toolkit for schools (2018) https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

[142] defenddigitalme (2020) The ICO Age Appropriate Design Code and schools https://defenddigitalme.org/2020/09/the-ico-age-appropriate-design-code-and-schools/

[143] Ekambaranathan, A., Zhao, J. and Van Kleek, M (2020) Understanding Value and Design Choices Made by Android Family App Developers. CHI'2020. Extended Abstracts, April 25–30, 2020, Honolulu, HI, USA. https://dl.acm.org/doi/10.1145/3334480.3383064

1.4.4 Parental access to a child's educational information

The House of Commons July 2016 briefing paper CBP-7657 considers parental responsibility and access to pupil records.[144]

Parents may be recognised differently under education law than under family law. For the purposes of education law, section 576 of the *Education Act 1996* defines a 'parent' as:

- all natural (biological) parents, whether they are married or not;
- any person who, although not a natural parent, has parental responsibility for a child or young person (this could be a step-parent, guardian or other relative);
- any person who, although not a natural parent, has care of a child or young person.

A person has care of a child or young person if they are the person with whom the child lives and who looks after the child, irrespective of what their relationship is with the child.

In family law 'parental responsibility' means all the rights, duties, powers, responsibilities and authority which by law a parent has in relation to the child. People other than a child's natural parents can acquire parental responsibility, for example through being appointed a guardian or adopting a child. More than one person can hold and exercise parental responsibility for a child.

Education law gives parents the right to information about their child's education. However, these rights differ depending on the type of school the child attends. In all cases a parent can access information about their child's education where the child is below the age of capacity, or where the child agrees, through a Subject Access Request under UK data protection law.

In addition, the Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437) give parents of pupils at Local Education Authority (LEA) maintained schools the right to access their child's educational records. Educational records may include information such as the records of the pupil's academic achievements as well as correspondence from teachers, local education authority employees and educational psychologists. Parents have a right to access their child's educational record, even if their child does not wish them to access it. This applies until the child reaches 18.

The Education (Pupil Information) (England) Regulations 2005 do not apply to non-maintained schools (e.g. academies, free schools and independent schools). This means that parents have fewer rights to access their child's educational records than parents in Local Education Authority maintained schools. Instead, the Education (Independent School Standards) Regulations 2014[145], which came into force on 5 January 2015, set out certain minimum standards that all independent schools (including academies and free schools) must meet.

The standards on information provision require that an annual written report of each registered pupil's progress and attainment in the main subject areas taught is provided to the parents of that registered pupil. This could offer an ideal place to expand upon the duty to include a list of all data processing and third-parties that are engaged by the school. Where this happens today, is the exception.

Schools also have the right to refuse a parent's request for information in some circumstances; for example, where the information might cause serious harm to the physical or mental health of the pupil or another individual.

New legislation should adjust these discrepancies and introduce fairness across all kinds of educational settings.

[144] House of Commons Briefing Paper | July 2016 | Schools: Parental Decision Making and Access to Pupil Records CBP-7657 https://commonslibrary.parliament.uk/research-briefings/cbp-7657/

[145] The Education (Independent School Standards) Regulations 2014 (SI 3283/2014) http://www.legislation.gov.uk/uksi/2014/3283/made

1.4.5 Then the children became data

The summer of exams 2020 drew attention to the problems faced by children when their needs are prioritised less as individuals and instead public bodies prioritise the protection of the system.

Families fighting for EHC plans or school places for their child with additional needs in austerity[146] have felt this for a long time. Many in the Traveller community or other marginalised groups have felt the stigma of data labels applied as part of a cohort. The harmful effects of standardisation is not new for the third of children held back by a failed system of comparable outcomes that leave school without any good exam grades in a system that demands one third fail no matter how clever they all are. But we may be on the cusp of greater societal understanding after those harms became mainstream in and more for a wider range of white middle class children, in A-level and other results, who objected to decisions about their lives to be based on historical data over which they have no control.[147]

If you are profiled and targeted for interventions as a child in a Troubled Family again and again across public services, you experience negative feedback loops. The moral and political values embedded in those data are not neutral. That dataset tends to be the lead data for other linked datasets in children's social care predictive analytics, and again, the same factors are reinforced. There appears to be little appetite to tackle this at regional or national level as long as the data continue to give the answers that the policy seeks to find. But when "on average, if the model identifies a child is at risk, it is wrong six out of ten times. The model misses four out of every five children at risk. None of the models' performances exceeded our pre-specified threshold for 'success',"[148] it is overdue to end the use of those bad datasets and tools based on them that don't work and that have "dangerous blind spots" in life and death situations for children.

Generally, statistical research may imply that the result of processing for statistical purposes is not personal data, but national uses of administrative pupil data for loosely defined research purposes have been allowed to overstep this for so long at local and national levels that it is now used for individual interventions. It will be the death knell of datasets for longitudinal public interest research.

The key take away from this report should not be how much data is collected about a child although it may be the most striking. It is not our aim to highlight theoretical risks or abstract concept of privacy. Instead, it is to demonstrate what has happened in England's education system as we have enabled the datafication[149] of children as individuals, and exclusion and "managed moves" of outliers —the disabled, the lower achieving and those who won't get good grades —as to quote Michael Rosen, "the children only learnt what could be turned into data. Then the children became data."[150]

Children's outcomes and everyday lives have become mechanistic targets as part of a cohort— behaviour points, absence scores and reading for pleasure at school level— and in turn schools are forced to turn the complexity of children's lives into simplified progress scores or attendance ratings

[146] Parveen, N. (2019) The Guardian | Funding for pupils with special educational needs drops 17% North of England has been worst hit, report finds, with funding down 22% since 2015 https://www.theguardian.com/education/2019/apr/04/funding-pupils-special-educational-needs-send-drops-north-england

[147] Burgess, M. (Wired) The lessons we all must learn from the A-levels algorithm debacle https://www.wired.co.uk/article/gcse-results-alevels-algorithm-explained

[148] What Works for Children's Social Care (2020) Machine Learning in Children's Services: Does it work? https://whatworks-csc.org.uk/research-report/machine-learning-in-childrens-services-does-it-work/

[149] Lupton, D. and Williamson, B (2017) The datafied child: The dataveillance of children and implications for their rights. New Media & Society doi: 1461444816686328.

[150] Michael Rosen (2018) The Data have Landed http://michaelrosenblog.blogspot.com/2018/02/the-data-have-landed.html

without context, to be ranked and spanked in league tables by the national Regulator. Children's lifetime educational achievement is now measured through the lens of the Treasury. What kind of world will they grow up in, if all of education and aspirations are only given value measured by what LEO says?

The developing child must be permitted to make mistakes and not have them permanently recorded and distributed indefinitely to others simply because the data systems make it possible. Their historic data must not be held against them. Historic data can cause harm.

To move forward and level up the edTech playing field we need a model of education that prioritises access, inclusion, safety, privacy, and young people's views[151] in how their own data is used underpinned by the public interest that safeguards the delivery of trustworthy systems.

If a child is denied entrance into the university of their choice, parents may wonder if their children's Prevent profiles[152] were passed on to institutions and used to screen and reject their application.

If their children are turned down for jobs, did the employer's screening app check them out using an online profile of their social media or browsing history gathered by their school-issued device and bought from data brokers?

If children's identities are stolen, was it the result of an app data breach many years ago?

If children are denied public services as an adult, could it be because of their records held by the National Department for Education or other agencies?

These are the kinds of questions that East German residents found had become very much a reality in the years of the secret use of pupils' and other personal records of the State Security Service of the former GDR only once it was made accessible to the public after 1989.[153]

When police start to repurpose school records for criminal investigation, the Department for Work and Pensions seek fraudulent benefit claimants in every child that went to school, or the Home Office has free rein on repurposing national school records to deny Early Years children a free school meal there are three things seriously wrong.[154]

The authorities attitude towards how they treat children's data, reveals how they treat people:

- Authorities have begun to act outside the law through lack of regulatory enforcement.
- The Department for Education has not only lost sight of its data but its purpose.
- Government policy has chosen to put punitive measures ahead of children's wellbeing and rights to private and family life.

It is our aim for this research to contribute towards change.

Overleaf. Fig 3. The legislation and data items expanded in the national pupil database.

[151] Coleman, S., Pothong, K., Vallejos, E.P and Koene, A. (2017) The Internet on our Own Terms: How children and young people deliberated about their digital rights | University of Nottingham, Horizon Digital Economy Research, 5Rights

[152] Grierson, J. (2020) The Guardian | Manchester colleges agreed to share data of students referred to counter-terror scheme https://www.theguardian.com/uk-news/2020/jul/19/manchester-colleges-agreed-to-share-data-of-students-referred-to-counter-terror-scheme

[153] The Federal Commission for the Records of the State Security Service of the former GDR https://www.bstu.de/en/the-stasi/the-unofficial-collaborators-of-the-mfs/

[154] FOI request to the Department for Education (July 2020) Pupil data and Workforce data: Home Office and Policing data cooperation https://www.whatdotheyknow.com/request/pupil_data_and_workforce_data_ho#incoming-1630439

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

the Education (Pupil Information) (England) (Amendment) Regulations 2018

The Education (Pupil Information) (England) (Amendment) Regulations 2019 amended the Education (Pupil Information) (England) Regulations 2005 (S.I. 2005/1437)

The Education (Information About Individual Pupils) (England) (Amendment) Regulations 2020

"such individual pupil information as may be prescribed"

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

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

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

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

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

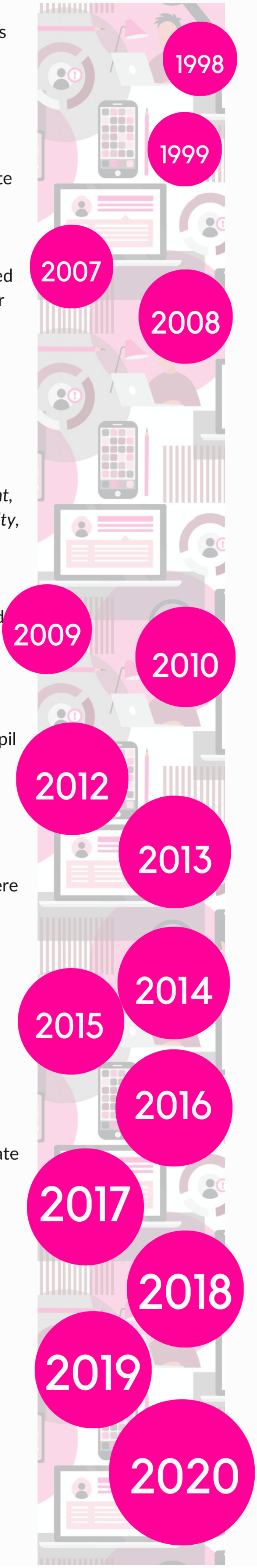
SEND primary and secondary need of those types if there is more than one type. Whether statement or an Education, Health and Care plan in place.

Small Business, Enterprise and Employment Act 2015 (Destinations data for linkage of all of this data with Longitudintal Educational Outcomes - the LEO dataset)

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

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

CIN census expanded.



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

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

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

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

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

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

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

Information to be included in the head teacher's report to parents for pupils with special educational needs in key stage 2 must include the pupil's assessment in English and mathematics and remove the reporting requirement for science.

The results of all national curriculum assessments to be added to a pupil's common transfer file, whether those assessments are taken at the end of a key stage or otherwise.

Reasons for absence and the total number of morning and afternoon sessions missed.

1.5 Further work

This concludes Part 1 of this work: A summary report of recommendations and main findings. The further parts can be found online at:

https://defenddigitalme.org/the-state-of-data-2020/

Part 2: National statutory data collections age 0-25 (standardised testing and censuses)
Part 3: Local data processing with case studies of commonly used edTech products
Part 4: The transition year from compulsory school to Higher Education
Part 5: Annex of data, source materials, research and references.

Acknowledgements

Funded by the Joseph Rowntree Reform Trust and report distribution costs are supported by the Charity Pot at LUSH.

The views contained in the report reflect solely the opinion of the author, Jen Persson. The author would like to thank the following for their direct and indirect input, contributions and support.

All our defenddigitalme Advisory Council members plus Alex Haydock | Alice Bradbury | Ailidh Callander | Andrew Cormack | Ann Marie Christian | Audrey Watters | Ben Williamson | Big Brother Watch | Bob Harrison | Borja Moya | Bukky Yusuf | Daragh O'Brien | The Digital Freedom Fund | Doug Levin | Ed Tranham | EDRi | Edugeek forum staff, poll respondents and members | Elizabeth Wright | Emmeline Taylor | FIPR | Gail Myerscough | Heather Burns | Huw Davies | Ivana Bartoletti | Joanna Redden | Jody Moore | Joshua Perry | Leo Ratledge | Liberty | Lydia Hill | Madeleine Holt | medConfidential | Miranda Prynne | MoreThanAScore | Nadia Snopek | Nadine Bernard | Nani Jansen Reventlow | Neil Selwyn | Privacy International | Rachel Mewes | Raphaëlle Heaf | Richard White | RightsWatch UK | Sarah Chesney | Second Home Studios animation | Selena Nemorin | Sonia Livingstone | Tamasin Cave | The staff and young people of the Warren Youth Group, Hull | Toks Oladuti | Trudy Mensah | Zoetanya Sujon and to everyone I've not mentioned by name including all the company CEOs and staff who contributed information about their products or experiences; the anonymous contributors, third-sector and civil society organisations, school staff, union staff, parents, and young people's stories, shared over the last four years at The BETT show, Schools and Academies Shows, ResearchED, Headteachers' Roundtable, Festival of Education, or WomenEd or those who generously invited me to their offices, schools, or reviewed the report.

A special thank you goes to Chandrima Chattopadhyay and Emilie Rabot for their dedicated research contributions into technology privacy policies and university data analytics, and all our other student research volunteers, as well as Alice Bradbury and Ben Williamson for their direct contributions.

Our appreciation also goes to the Freedom of Information Officers and staff in government departments, schools, local authorities, and universities that responded to our requests for information, staff at the ICO, and all of the unnamed education sector staff that helped us understand local practice and systems.

Jen Persson
Director, defenddigitalme

> “This comprehensive report deserves close reading by all those concerned with children’s privacy and security. Ministers and officials in the Department of Education and government would do well to consider its detailed recommendations that reveal both a gross injustice for an entire generation of children, and usefully signpost the way forward.”

Baroness Beeban Kidron, Chair, 5Rights Foundation

defend children's privacy.

defend children's digital rights.

defend digital me.

defend|digital|me

Cover illustration pattern art by Gail Myerscough https://www.gailmyerscough.co.uk/
Big Data Wheel illustration, icons and national pupil data lifetime CV by Nadezhda Snopek
Accompanying animation by Second Home Animation Studios https://www.secondhomestudios.com/

defenddigitalme.org