

**NGO submission for the List of Issues Prior to Reporting (LOIPR) for the 88<sup>th</sup> pre-session State Reporting Procedure on the Implementation of the UN Convention on the Rights of the Child in the United Kingdom of Great Britain and Northern Ireland (UK)**

defenddigitalme



October 31, 2020

## Table of Contents

<b>1. Background</b>	<b>3</b>
<b>2. Introduction</b>	<b>3</b>
<b>3. National Pupil Data Collection by the State</b>	<b>5</b>
3.1 The National Pupil Database	5
3.2 National Pupil Database expansion legislation for children age 5-19	7
3.3 National Pupil Database expansion of re-use for other purposes	9
3.4 National Pupil Database expansion from Higher Education	9
3.5 Proposed questions on national pupil data	10
<b>4. State surveillance in schools for the Prevent programme</b>	<b>10</b>
4.1 The Prevent program and the power imbalance for children	11
4.2 Local surveillance using computer monitoring technology	14
4.3 Private companies provide monitoring technology and control practice	15
4.4 State transfers of data from compulsory education to Higher Education	16
4.5 Proposed questions on the Prevent programme and child surveillance	16
<b>5. Public sector outsourcing of educational activity to private sector actors through edTech and research</b>	<b>17</b>
5.1 National funding of product trials and commercial research using children	17
5.2 National funding of research trials using children	18
5.3 Proposed questions on research and product trials in education	19
<b>6. Children's social care use of big data and machine learning</b>	<b>19</b>
6.1 Informed consent	20
6.2 Proposed questions on predictive algorithms in children's social care	21
<b>7. Training and communications on privacy and rights for the classroom</b>	<b>21</b>
7.1 Children's views on their own data and privacy	22
7.2 Proposed questions on education about digital rights	22

# 1. Background

1. This submission is for consideration under the grouping *Civil rights and freedoms* and specifically *the protection of privacy (art. 16), the right to seek, receive and impart information (art. 13) and freedom of thought, conscience and religion (art. 14)* but also has implications for the Right of the Child to be Heard (Article 12) and their best interests (Art.3)
2. This submission has been prepared by defend digital me, (hereafter “defenddigitalme”). defenddigitalme is a call to action to protect children’s rights to privacy. We are teachers and parents who campaign for safe, fair and transparent data processing in education, in England, and beyond. We advocate for children’s data and digital rights, in response to concerns about increasingly invasive uses of children’s personal information. defenddigitalme is a call to action to protect children’s rights to privacy and family life. We are working towards safe, fair and transparent data, as part of our vision of a rights’ respecting environment in state education. We began work in 2015 and the organisation was formally founded in 2017 as a not-for-profit company limited by guarantee with charitable objectives, funded by the Joseph Rowntree Reform Trust.<sup>1</sup>
3. We monitor State policy and legislation in the remit of the Department for Education (hereafter “The DfE”) in England and Wales, as well as where the use of data collected in the state education system is used elsewhere in government, and by private stakeholders and commercial third parties. The DfE in England and Wales is responsible for both education (in certain aspects where it is not devolved) and children’s social care. At the time of writing we are in the process of publishing a comprehensive report with recommendations, having researched a child’s digital footprint in the state education landscape in England, *The State of Data 2020*.<sup>2</sup>
4. This submission’s scope is the effect of the state education system in England on children’s rights to privacy and family life, as a result of national State data collections, and the State use of children’s personal data collected in education for other non-educational purposes including a) immigration enforcement and b) the purposes of the Prevent programme, as part of the Counter-Terrorism and Security Act 2015<sup>3</sup> duty on specified authorities to have due regard to the need to prevent people from being drawn into terrorism. We also address the public sector use of private actors in educational technology (hereafter “edTech”), and the implications for children’s range of rights. Furthermore, we draw attention to the use of data and technology in children’s social care, and in particular the use of predictive algorithms.

# 2. Introduction

5. The general situation which has an impact on the implementation of the UNCRC in relation to children’s human rights and freedoms has worsened considerably since

---

<sup>1</sup> The Joseph Rowntree Reform Trust Ltd <https://www.jrtrt.org.uk/>

<sup>2</sup> The State of Data 2020: Mapping a child’s digital footprint in the state education landscape in England <https://defenddigitalme.org/the-state-of-data-2020/>

<sup>3</sup> The Counter-Terrorism and Security Act 2015 contains a duty on specified authorities to have due regard to the need to prevent people from being drawn into terrorism. This is also known as the Prevent duty. <https://www.gov.uk/government/collections/counter-terrorism-and-security-bill>

the last Review. The 2019 mid-term Review by the Children’s Commissioner focussed on the child protection aspects of children’s online lives, and as standalone ‘bolt on’ digital rights<sup>4</sup>, rather than children as holders of all of the relevant rights as may be affected in digital aspects of their lives and its administration by the State.

6. Not only does the Government fail to meet its commitment to assess fully the impact of its data policies and changes in legislation on the rights of all children, but some policies are hostile to children by design. Recent response to digital provision in COVID-19 has been dire and recently cut, not increased.<sup>5</sup>
7. The report by the Joint Committee on Human Rights on the UK’s compliance with the UN Convention on the Rights of the Child, Eighth Report of Session 2014–15 stated, *“If all government departments were required to take the trouble to consider how their legislation is compliant with the UNCRC articles and to report on that assessment to Parliament, that would constitute a very necessary, and significant, step towards making those departments more aware of their duties under that Convention.”*<sup>6</sup>
8. The Council of Europe 2016-21 Strategy on the Rights of the Child<sup>7</sup>, 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.”*
9. 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.”*<sup>8</sup>
10. Despite Ministerial statements and clear spoken commitment that the Government will give due consideration to the UNCRC articles when making new policy and legislation this has not been realised. The DfE fails to demonstrate in its actions as regards national pupil data handling that it always has the best interests of the child or any recognition of its obligations to realise child rights at the heart of all of its actions.

---

<sup>4</sup> UK Children’s Commissioners’ UNCRC mid-term review (2019)  
<https://www.childrenscommissioner.gov.uk/report/uk-childrens-commissioners-uncrc-mid-term-review/>

<sup>5</sup> BBC (October 2020) Covid: Laptop allocation for deprived pupils cut at some schools  
<https://www.bbc.co.uk/news/education-54675620>

<sup>6</sup> The UK’s compliance with the UN Convention on the Rights of the Child - Human Rights Joint Committee (2014-15)  
<https://publications.parliament.uk/pa/jt201415/jtselect/jtrights/144/14405.htm>

<sup>7</sup> Council of Europe Strategy for the Rights of the Child 2016-21 Para 37, p15/36 <https://rm.coe.int/168066cff8>

<sup>8</sup> 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](https://www2.ohchr.org/english/bodies/crc/docs/GC/CRC-C-GC-16_en.doc)

### 3. National Pupil Data Collection by the State

11. Children in England have lost control of their digital footprint by their fifth birthday simply by being part of the state education system. The State fails to take any account of children's right to privacy (Art. 16), or children's right to be heard (Art.12) when it comes to their personal data processing in the state education sector.
12. The Information Commissioner's Office (ICO) recently published the outcome of a compulsory and wide-ranging audit of the DfE<sup>9</sup> undertaken in response to our regulatory complaint on the handling of national pupil data, and subsequent complaints by Liberty on DfE data sharing with the Home Office for the purposes of immigration enforcement.
13. The audit found that data protection was not being prioritised and this had severely impacted the DfE's ability to comply with the UK's data protection laws. The DfE are not fulfilling their duties that data "shall be processed lawfully, fairly and in a transparent manner." A total of 139 recommendations for improvement were found, with over 60% classified as urgent or high priority.
14. The Department itself needs systemic and structural change and independent oversight, after the 2020 ICO compulsory audit found it was failing to process data in a fair, lawful and transparent way. The DfE gives away millions of children's sensitive and identifying records and yet the ICO found that, "the Commercial department do not have appropriate controls in place to protect personal data being processed on behalf of the DfE by data processors."
15. An Assessment Notice was issued to the DfE on 19 December 2019. The audit field work was undertaken at DfE Offices in London, Coventry, and Sheffield between 24 February and 4 March.

#### 3.1 The National Pupil Database

16. The National Pupil Database<sup>10</sup> is a collection of around twenty-five different and linked data collections across the school year, from children age 0-25 through their educational settings.
17. In 2012 government Ministers decided to change the law<sup>11</sup> to give away millions of children's identifying school records, for commercial reuse among other purposes.
18. Over 21 million people's names are now in the national pupil database, collected since 1996, with special educational needs, even university applicants' religion and sexual orientation from equality monitoring. But the ICO audit identified that the DfE doesn't have a good grasp of everything it holds.

---

<sup>9</sup> ICO Statement on the outcome of the ICO's compulsory audit of the Department for Education (October 2020) <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/>

<sup>10</sup> The National Pupil Database [https://en.wikipedia.org/wiki/National\\_Pupil\\_Database](https://en.wikipedia.org/wiki/National_Pupil_Database)

<sup>11</sup> Call to review pupil data law <https://defenddigitalme.org/call-to-review-relevant-legislation/>

19. *“There is no clear picture of what data is held by the DfE and as a result there is no Record of Processing Activity (ROPA) in place which is a direct breach of Article 30 of the GDPR.”*
20. The ICO clearly identifies that the requirement for a ROPA has been documented for over a year in audit reports and meeting minutes, however little progress has been made to address this. The DPO has been doing a good job. The accountability rests much higher up.
21. Children’s confidential data is collected simply because they go to school. Without parents’ permission it is given away and used for profit, misused by other government departments and in 2020 the press revealed that learner data was being misused by gambling companies<sup>12</sup> for ID verification, to onboard new gamblers.
22. Article 14 requires that States Parties shall respect the rights and duties of the legal guardians, and where applicable, to provide direction to the child in the exercise of his or her right in a manner consistent with the evolving capacities of the child.
23. Our commissioned poll of over 1,000 parents in 2018<sup>13</sup> showed over 69% of parents asked, hadn’t heard of the National Pupil Database and did not know that children’s personal data could be passed out from it by the State to third parties.
24. We need information and action from the Department in order to meet this obligation, as well as adequate remedy for infringement of children’s rights Article 16.
25. The full audit has not been released. We are working towards this aim in the public interest, at the time of writing. Key findings from the ICO audit summary include:
  - *“The Commercial department does 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.”*
  - *“The DfE are providing very limited training to staff about information governance, data protection, records management, risk management, data sharing, information security, individual rights and in some cases there is no assurance that staff are receiving any training whatsoever.”*
  - *“The DfE are reliant on third parties to provide privacy information on their behalf however, this often results in insufficient information being provided and in some cases none at all which means that the DfE are not fulfilling the first principle of the GDPR, outlined in Article 5(1)(a), that data shall be processed lawfully, fairly and in a transparent manner.”*
  - *“There is no formal proactive oversight of any function of information governance, including data protection, records management, risk management, data sharing and*

---

<sup>12</sup> The Times (January 2020) Revealed: betting firms use schools data on 28m children  
<https://www.thetimes.co.uk/article/revealed-betting-firms-use-schools-data-on-28m-children-dn37nwg5>

<sup>13</sup> 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>  
 The State of Data survey was carried by Survation commissioned by defend digital me, between 17th and 20th February 2018. Survation polled 1,004 parents’ opinions of children’s data collection and uses of everyday technology in state education. Respondents were parents of state-educated children aged 5-18 in England.

*information security within the DfE which along with a lack of formal documentation means the DfE cannot demonstrate accountability to the GDPR.”*

- *“In 400 applications, only approximately 12 were rejected due to an approach which is designed to find a legal gateway to ‘fit’ the application rather than an assessment of the application against a set of robust measures designed to provide assurance and accountability that the sharing is lawful in line with statutory requirements.”*

### 3.2 National Pupil Database expansion legislation for children age 5-19

26. Data must only be submitted by schools to the national government for educational purposes under s537a of the Education Act 1996. There is inadequate oversight of national pupil data legislative change and the current process means that children's rights are easily ignored when laws are changed to give the government greater powers to collect more named data about each child in state education without adequate scrutiny.<sup>14</sup>
27. Cumulative changes to laws without active scrutiny (through the negative statutory instrument process)<sup>15</sup> by successive governments up to and including the 2012-3 changes to the Education Act 1996<sup>16</sup>, and Prescribed Persons Act 2009, have enabled the release of individual and sensitive data to a broad range of external third parties, narrowly, *“for the purpose of promoting the education or well-being of children in England.”*
28. The DfE expanded the school census in October 2016 to start collecting nationality and country of birth on every child in England in state education (8 million children every year), The full details are published in our timeline of the school census nationality data expansion.<sup>17</sup> It was highly controversial and ended in June 2018.
29. In 2017 the government introduced another expansion, via negative [Statutory Instrument 807/2017](#) The Education (Information About Children in Alternative Provision) (England) (Amendment) Regulations 2017. The [Explanatory Note](#) gives no explanation of the itemised content and sensitivity of the *reasons for placement* (transfer out of mainstream into Alternative provision education) including highly sensitive reasons ascribed by the Local Authority such as pregnancy / child care, youtube offender and detailed health needs. There was no effort made to inform the families of the children this data collection was about, about the new national data.<sup>18</sup>
30. 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

---

<sup>14</sup> The making of a very bad law: school census nationality data one year on (2017) <https://defenddigitalme.org/2017/07/the-making-of-a-very-bad-law-school-census-nationality-data-one-year-on/>

<sup>15</sup> For the list of Statutory Instruments that have incrementally expanded which data can be collected on children since 1996, and on a named basis, 2002-17, see Annex to question HL2783. <https://questions-statements.parliament.uk/written-questions/detail/2017-11-01/HL2783>

<sup>16</sup> The Education Act 1996 (s537a) [www.legislation.gov.uk/ukpga/1996/56/section/537A](http://www.legislation.gov.uk/ukpga/1996/56/section/537A)

<sup>17</sup> School census expansion (2016) timeline <https://defenddigitalme.org/timeline-school-census/>

<sup>18</sup> Timeline of the Alternative Provision Census expansion (2017) <https://defenddigitalme.org/timeline-alternative-provision/>

whether their child was “Italian”, “Italian-Sicilian” or “Italian-Neapolitan”. The BBC reported the Ambassador pointed out Italy has been a unified country since 1861.<sup>19</sup>

31. In October 2016 we discovered that national pupil data had been used in secret for Home Office immigration enforcement purposes since July 2015. Those monthly national pupil data handovers between the DfE and the Home Office continue.<sup>20</sup> This means that children’s personal details such as home address from up to the last five years, and full names and school address, which are submitted in good faith by schools for the purposes of pupil administration and school funding to the DfE, are actually being used by other government departments for other reasons.
32. In July 2016 in a written parliamentary question<sup>21</sup>, the Schools Minister said of nationality and country-of-birth that, “The data will be collected solely for internal Departmental use for the analytical, statistical and research purposes ... There are currently no plans to share the data with other government Departments”.
33. However the live data sharing agreement had already been written and was active between the two government departments, but was not yet public. It included the agreement that “nationality (once collected)” in the information to be transferred between the Home Office and DfE for purposes including the strategic aims of the Hostile Environment.<sup>22</sup> Monthly handovers of data from the DfE to the Home Office for these purposes continue under a since amended version of the agreement.
34. There is no public information available on the outcomes for children from the use of the data. The Home Office has declined<sup>23</sup> to provide any transparency of what happens to children as a result of the Home Office being given personal data from 1545 children’s school records in the five years between July 2015 and July 2020. When asked by a Member of Parliament, the Department replied that “The specific information you have requested is not readily available and could only be obtained at disproportionate cost.”<sup>24</sup>
35. School children’s census data continues to be handed over to the HO every month. Including explicitly to “create a hostile environment.” As a result of these policies we see:
  - Harm to children as young as 10 whose [confidentiality was breached](#) when asked for countries of origin in front of peers in the classroom, without parental consent; and [pupils who were not white British were told to send in birthplace data](#).

---

<sup>19</sup> BBC (2016) UK school pupil ethnicity question angers Italy <https://www.bbc.co.uk/news/blogs-news-from-elsewhere-37631062>

<sup>20</sup> DfE external data shares <https://www.gov.uk/government/publications/dfe-external-data-shares>

<sup>21</sup> Parliamentary question 42842 <https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-07-15/42942/>

<sup>22</sup> Data sharing agreement with reference to paragraphs 15.1.2 and para 15.2 .6 <https://www.whatdotheyknow.com/request/377285/response/941438/attach/4/20151218%20DfE%20HO%20Final%20V0%201%20REDACTED.PDF.pdf>

<sup>23</sup> Home Office Freedom of Information request refused [https://www.whatdotheyknow.com/request/departement\\_for\\_education\\_pupil\\_d](https://www.whatdotheyknow.com/request/departement_for_education_pupil_d)

<sup>24</sup> Parliamentary question UIN 92745 asked by Caroline Lucas MP of the Home Office <https://members.parliament.uk/member/3930/writtenquestions?page=3#expand-1236241>

- Harm to children who have been withdrawn from education as a result. No one knows how many, but we know of some through charities supporting children since.
  - Harm to the relationship between parents and schools as [sanctuaries of learning](#)
  - Harm to professional trust in politicians and policy makers
  - Harm to public trust in the legislative process and new lawmaking
36. During the development of the UK Data Protection Act 2018, the government put an exemption into law which [a government Minister](#), explained explicitly planned for national pupil data to be exempt from data protection law and will be used for by the government, to embed the secret policy that had been put in place in 2015, that went undiscovered for a year until we exposed it.
37. Departmental assurances are now insufficient that the nationality data collected between 2016 and 2018 will not be misused, when compared with what can be done based on the legislation and current policy. We are seeking its destruction.
38. One need only look at some politicians' attitudes towards [Roma](#), and the U.S. practice on child separation and immigration, to understand that the DfE England holds data that poses a serious risk of harm. It is profoundly naive to think that any future policy or government might not use children's data in England similarly.

### 3.3 National Pupil Database expansion of re-use for other purposes

39. In April 2018 DfE permitted the use of the National Pupil Database for a DWP benefit fraud investigation of 185 children.<sup>25</sup>
40. 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 instead by using the national pupil database.<sup>26</sup>
41. These purposes are in our opinion unlawful since the data were not collected for such purposes and families have not been told their school children's data may be used for this.

### 3.4 National Pupil Database expansion from Higher Education

42. The 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.<sup>27</sup>
43. Young people who apply to university in the UK may be aged 17 (or in exceptional cases younger) at the time of application. Equality Monitoring data from applicants to

---

<sup>25</sup> Pupil data and Workforce data: Home Office, Policing and Fraud investigation reuse of pupil data [https://www.whatdotheyknow.com/request/pupil\\_data\\_and\\_workforce\\_data\\_ho#incoming-1630439](https://www.whatdotheyknow.com/request/pupil_data_and_workforce_data_ho#incoming-1630439)

<sup>26</sup> *ibid.*

<sup>27</sup> Statement on student religion or belief, and sexual orientation data in the National Pupil Database (July 2019) <https://defenddigitalme.org/2019/07/statement-on-student-religion-or-belief-and-sexual-orientation-data-in-the-national-pupil-database/>

Higher Education are passed on from UCAS and universities to the private body, [HESA, the Higher Education Statistics Agency Ltd](https://www.hesa.ac.uk/).<sup>28</sup> HESA passes sensitive and personal confidential information on to other funding bodies. This data now sits on a named basis in multiple national databases, including [the National Pupil Database](#) at the DfE 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.

44. For many worthy reasons, many organisations advocate for the collection of [religion](#) or [sexual orientation](#)<sup>29</sup> among equality monitoring data. But any risk of loss, theft, leak or misuse could be devastating to individuals and communities. Risk of damage or distress is high.
45. There can be no justifiable necessity for distribution of named data in this way that is proportionate to the risks to fundamental rights and freedoms.

### 3.5 Proposed questions on national pupil data

46. The ICO summary audit stated the DfE accepted all the audit recommendations and is making the necessary changes. In order for children and their families to be made aware of how their rights have been infringed and what remedy is available to them
  - a. Will the Department publish the full findings including what was found unlawful in the ICO audit of the DfE?
  - b. By when must the Department undertake which actions?
  - c. What will the Department do in order to inform every family of how their child's data is being given to commercial companies, think tanks, and the press?
  - d. Will the Department make a meaningful Ministerial commitment to give due consideration to the UNCRC when developing law and policy with regard to national pupil data collection and how will it be overseen?
  - e. Will children's nationality and country of birth data collected between 2016 and 2018 be destroyed since it is not being used for the purposes of its collection?
  - f. Will the Department for Education commit to change the process of collecting Higher Education applicants' equality monitoring data anonymised at source, not named and if not, why not?
  - g. Given that the DfE has broken the law on children's rights to privacy as well as data protection, what will the government do to hold itself accountable for real change in future?

## 4. State surveillance in schools for the Prevent programme

47. The policy of the Prevent programme towards children in educational settings has significant and lasting effects on children for their full and free development unimpeded by interference from the State into adulthood. With effects on privacy

---

<sup>28</sup> HESA <https://www.hesa.ac.uk/>

<sup>29</sup> HESA (data types on sexual orientation) <https://web.archive.org/web/20190726172535/https://www.hesa.ac.uk/collection/c18051/a/sexort>

(article 16), the right to seek, receive and impart information (article 13) and freedom of thought, conscience and religion (article 14).

48. The purposes of the Prevent programme are by definition to subject children to interference with his or her privacy, family, home or correspondence, many interferences result in harm to his or her honour and reputation.

#### 4.1 The Prevent program and the power imbalance for children

49. In 2019, a legal settlement was reached following court action by the family of a primary school-aged child which will see all the child's records removed from the Prevent anti-radicalisation records. *"Lawyers instructed to act for the parents and child, argued that the records could be used against the child in the future, as the Met police did not give any guarantee that the records wouldn't be included in any Disclosure and Barring criminal record checks when the child becomes an adult."*
50. *"The aim of Prevent is to pre-empt involvement in terrorism in people who have not yet committed an offence. Whilst external agencies such as the Home Office can request information from the database onto which Prevent officers in the police force enter people's details, individuals are not made aware that they are recorded. In this case the Met police was threatened with judicial review and agreed to settle and delete the child's details."* (Matrix Chambers, 2019)<sup>30</sup>
51. In a separate case in September 2020, *"the Court found that the retention of data by the Metropolitan Police Service on a 16-year-old child (known as II) from the age of 11 was unlawful and a disproportionate interference with his right to private life; namely, that it was a breach of his Article 8 right under the European Convention on Human Rights, as well as sections 35 and 39 of the Data Protection Act 2018."*
52. *Whilst the police case was closed in June 2016 due to no counter-terrorism concerns and no evidence of radicalisation, the Metropolitan Police Service nonetheless decided to retain the data. This resulted in the data being held across 10 separate databases, accessible to not only the police, but also local authorities and the Home Office. This is an important judgment that illustrates the unlawful exercise of police powers under the Prevent Strategy, which has been in existence since 2011."* (Deighton Pierce Glynn, 2020)<sup>31</sup>
53. *"The Claimant's mother said:*  
  
*"A dark cloud had loomed over my family for the past five years. My son had grossly misinformed allegations cast against him that could have had the potential to destroy his future. To constantly live, not knowing whether false information about your child, accessible by public bodies, would be shared, hampering his chance to live freely in a country you have always known to be home, is beyond heart-breaking. For us, this cloud passed, because we knew where and who to seek advice from, we*

---

<sup>30</sup> Child's records will be deleted from Prevent Case Management anti-radicalisation database (Matrix Chambers, 2019) <https://www.matrixlaw.co.uk/news/childs-records-will-be-deleted-from-prevent-case-management-anti-radicalisation-database/>

<sup>31</sup> Court finds data retention by the Metropolitan Police Service under the Prevent Strategy unlawful (2020) <https://dpglaw.co.uk/court-finds-data-retention-by-the-metropolitan-police-service-under-the-prevent-strategy-unlawful/>

*were guided by a brilliant legal team, but what about those who don't know?" (Deighton Pierce Glynn, 2020)*

54. Safeguarding-in-schools generated information, may be the trigger for staff to begin a Channel referral for children into the Prevent programme. 1 in 3 of all referrals come from the education sector today. The Home Office diagram of process flows below, set out the process, which starts with a Channel police practitioner screening the children referred.
55. 70% of referrals into the Channel programme in 2017-18, resulted in no action. Only 394 individuals received Channel support after the initial Channel panel discussion. MASH (Multi-Agency-Safeguarding-Hubs) can be secretive, and some have refused to disclose for example, even the privacy policy given to families<sup>32</sup>, or total numbers of children involved, although Channel participation is described as consensual and voluntary<sup>33</sup> it is not.

### 1.1 People referred to the *Prevent* Programme

In 2017/18, a total of 7,318 individuals were subject to a referral due to concerns that they were vulnerable to being drawn into terrorism. It should be noted that a number of terrorist attacks occurred in the month prior to and during the time period covered by this publication<sup>1</sup>, which will likely have had an effect on the number of referrals.

The sectors accounting for the highest number of referrals in 2017/18 were the **education** sector (2,462; 33%) and the police (2,364; 32%).

Of the 7,318 individuals **referred** to the Prevent programme in 2017/18, 3,096 (42%) left the process requiring no further action, 2,902 (40%) left the process and were signposted to alternative services prior to Channel discussions taking place, and 1,314 (18%) were deemed suitable, through preliminary assessment, to be discussed at a Channel panel.

Of the 1,314 individuals **discussed** at a Channel panel, 920 (70%) did not receive Channel support, and 564 (61%) of these individuals were referred to other services.

The remaining 394 individuals **received** Channel support following a Channel panel. Of these, 298 (76%) individuals have subsequently left the process, and 96 (24%) are currently still receiving Channel support. Of those who have left the Channel process, 251 (84%) did so with no further terrorism-related concerns. The remaining 47 (16%) individuals withdrew from the Channel process, although in some cases support from other services may still be in place and any terrorism risk that might be present is managed by the police.

### 1.2 Age

In 2017/18, of the 7,318 individuals **referred**, the majority (4,144; 57%) were aged 20 years or under. Those aged 20 years or under also made up the majority of the 1,314 individuals **discussed** at a Channel panel (818; 62%) and the 394 individuals that **received** Channel support (259; 66%).

Fig 1. Source: Home Office statistical bulletin 31/18 Individuals referred to and supported through the Prevent Programme, April 2017 to March 2018.

<sup>32</sup> FOI request to Brent council "The information is exempt from disclosure under Section 24 of the Freedom of Information Act (FoIA). Disclosure of the information poses a threat to the interests of national security; the information is being withheld in order to safeguard national security." [https://www.whatdotheyknow.com/cy/request/safeguarding\\_children\\_channel\\_an\\_5](https://www.whatdotheyknow.com/cy/request/safeguarding_children_channel_an_5)

<sup>33</sup> "Participation in Channel is voluntary and confidential and is not a criminal sanction." (2019) Prevent and Channel Factsheet <https://homeofficemedia.blog.gov.uk/2019/12/19/prevent-and-channel-factsheet/>

## DATA PROCESSING FLOW

March 2019

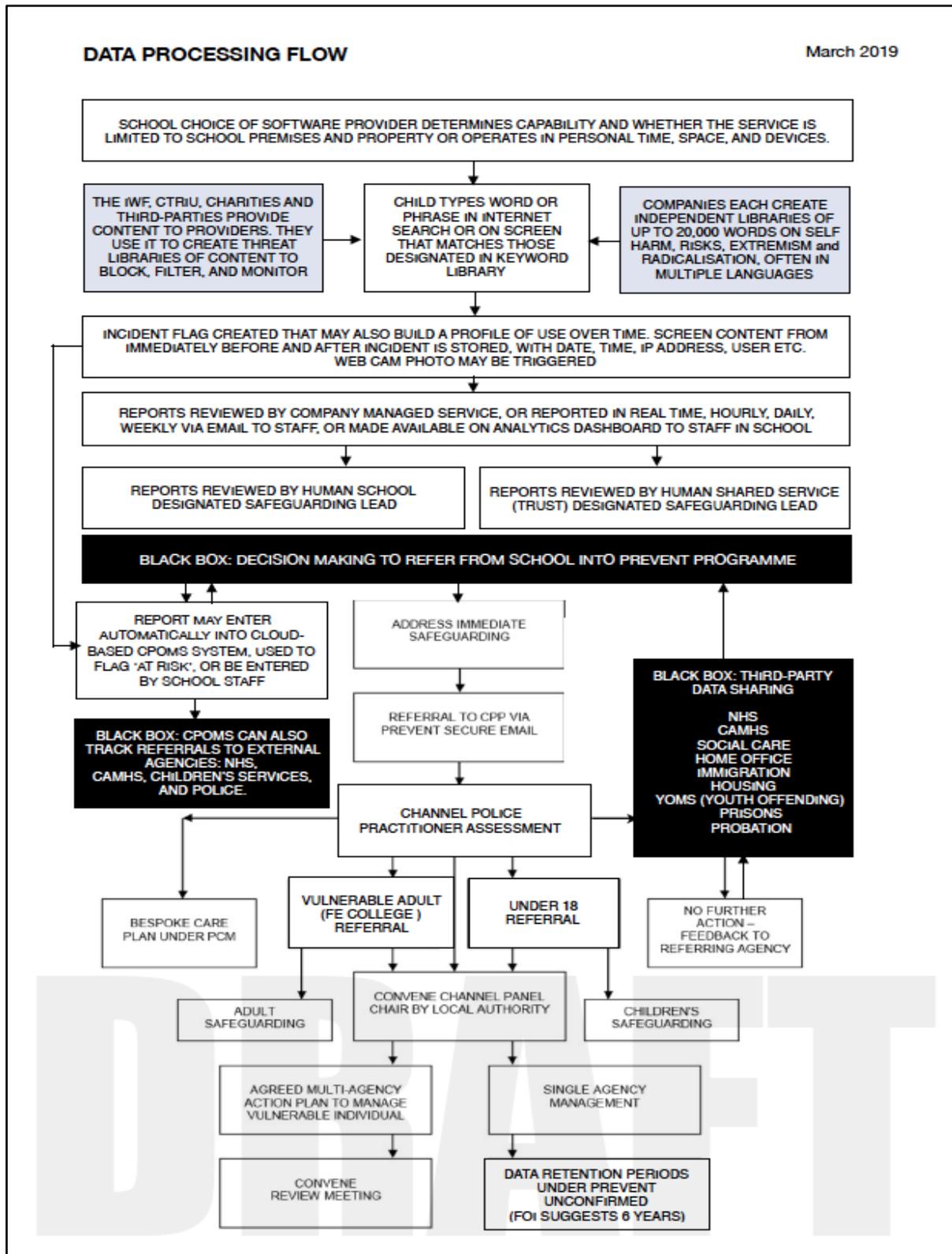


Fig 2. Diagram of estimated Prevent data flows about a school child. Source defenddigitalme

## 4.2 Local surveillance using computer monitoring technology

56. The DfE statutory guidance ‘Keeping Children Safe in Education’<sup>34</sup> 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.
57. A number of commercial providers of such services and software include terrorism as a category by which a child may find their Internet searches and computer activity labelled. 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. Defining safeguarding in schools services and software application standards could begin in the short term as consultation with industry and civil society, and lead to a statutory Code of Practice.
58. This is a challenging, complex area of data processing in the public sector, conflating important areas of safeguarding and child protection, with the politics of Prevent. It conflates age-old issues of bullying and social issues, with new issues of technology, outsourcing more commercial service providers in state schools and associated aspects of monopolies, mergers and competition, and opaque data practices.
59. Children must also be afforded the same opportunity consistently to have their concerns heard, when information is recorded about them through such tools, and to ask to be able to see, and for correction of their records. We are concerned about likely discrimination from the design choices made by companies and the providers of thousands of keywords that create the dynamic keyword libraries that trigger flags. We would like to see published rates of false flags, mistakes, common standards of statistical reporting especially when using non-English language and slang and on ethnicity, BYOD policies, and routes of redress for errors and their consequences.
60. The consequences of what happens after these many different systems trigger keywords is often entirely opaque to families, as our poll of parents in February 2018 showed, and we highlighted in this week’s blog. A poll of parents commissioned by defenddigitalme in February 2018 through Survation showed that 86% of parents with children in England’s state education system think that both children and parents should be informed of what the consequences are if these keywords are searched for, and 69% believe children should be told what these thousands of keywords are.
61. 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. The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child’s choice. This programme is detrimental to those aims in disproportionate ways at mass scale.

---

<sup>34</sup> 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>

62. The State should end the normalised surveillance of children under the Prevent Programme, and its chilling effects on freedom of speech, religion and privacy, 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 and creating individual profiles over time, and in particular any data storage abroad should be deleted.
63. 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."<sup>35</sup>

### 4.3 Private companies provide monitoring technology and control practice

64. While schools as public bodies should be accountable to children and their families, there is little route for accountability between private providers of such services and software. Private companies are also more susceptible to police access to the data they hold and without any transparent public accountability.
65. Regards data about a child created as a result of such monitoring, we have researched around 15 companies that operate in the sector. Their functionality is varied, but can include enabling webcam photos of the child to be taken without their knowledge. Triggering searches or on screen content may result in Prevent related labels being created about a child.
66. *"After NetSupport DNA's webcam capture feature has captured an image of the user, the image and any related incident data are processed in the usual safeguarding process and manner determined by the school. These may feed into the Channel / Prevent programme as and when appropriate following the school policy. NetSupport DNA is not responsible for the onward processing in further systems or by further third parties."*<sup>36</sup>
67. Products may monitor on-screen passwords and children's confidential counsellings services, and may pass on information that a child has typed on screen and subsequently chose to delete<sup>37</sup> as the CEO of Smoothwall explained to us in an interview in 2020. There is no oversight of companies' use of data after collection since they are not subject to Freedom of Information and any company may choose to decline to answer questions about how their product works, and its outcomes.

---

<sup>35</sup> 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>

<sup>36</sup> Case study on one provider that defenddigitalme has commented on in press and the challenges of doing so for NGO including legal threat <https://defenddigitalme.org/2018/12/netsupport-dna-complaint/>

<sup>37</sup> Safeguarding in schools: a Q&A discussion on practice, legal questions and child rights. With the CEO of Smoothwall and child rights experts [https://youtu.be/tMCS31\\_TrTY](https://youtu.be/tMCS31_TrTY)

68. At the House of Lords Communications Committee, (2016) the Managing Director, e-Safe Systems Limited, said:<sup>38</sup> “Bearing in mind we are doing this throughout the year, the behaviours we detect are not confined to the school bell starting in the morning and ringing in the afternoon, clearly; it is 24/7 and it is every day of the year. Lots of our incidents are escalated through activity on evenings, weekends and school holidays. Invariably, although the volume decreases, for example, during the six-week school holiday in the UK, the proportion of incidents which are very serious during that period is much higher.”

#### 4.4 State transfers of data from compulsory education to Higher Education

69. Manchester colleges and the DfE had an agreement to share data of students referred to the Prevent counter-terror scheme between further education colleges and Higher Education.<sup>39</sup> This has the potential to be a damaging precedent.
70. The arrangement, revealed in documents obtained in 2019 by the researcher Dr Hilary Aked<sup>40</sup>, involved the University of Manchester, the University of Salford, Manchester Metropolitan University, the University of Chester and the Manchester College, the largest further education college in the UK.
71. The Department later denied to us that an agreement existed involving the Department, although the Data Sharing Agreement listed it as a partner.<sup>41</sup>

#### 4.5 Proposed questions on the Prevent programme and child surveillance

72. Secrecy shrouds the Prevent programme and despite loud voices in its public outreach initiatives, the reality of transparency does not match the rhetoric. In order for children and their families to realise their rights when they have been infringed and to seek remedy, they need to go to court, which shows that the program is not consensual and such action is only open to a minority of those affected.
- h. Can the government provide figures on how many children have been referred to the Prevent programme in education, broken down by ethnicity?
  - i. Can the government explain why families must go to court to ask for records to be deleted if the Prevent programme is consensual?
  - j. Will the government make public its policy in relation to the national Prevent duty on monitoring school children’s computer activity at home?
  - k. Will the government end the monitoring of personal devices used by pupils?

---

<sup>38</sup> Lords Committee on Children and the Internet (2016) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/oral/41158.html>

<sup>39</sup> 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>

<sup>40</sup> See also Medact Report (2019) *False Positives: the Prevent counter-extremism policy in healthcare* <https://www.medact.org/wp-content/uploads/2020/07/MEDACT-False-Positives-WEB.pdf>

<sup>41</sup> Data Sharing Agreement Final v1.0 190109 <https://defenddigitalme.org/200415-data-sharing-agreement-2/>

- I. Will the government produce guidance on monitoring school children at home for schools and for families in order to know what their rights are and how they will be respected?

## 5. Public sector outsourcing of educational activity to private sector actors through edTech and research

73. 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.

### 5.1 National funding of product trials and commercial research using children

74. 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. 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.
75. 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 lifetime is not clear because it is not transparent to the family or recorded. 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. How much and which children are subjected to what kinds of interventions in their classroom or school-led activity at home is opaque. No single organisation appears to have oversight or be accountable for these activities.
76. 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.
77. 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.<sup>42</sup>

78. There is no mechanism for schools to consistently support families digital rights or route for making meaningful objections or when redress is required.

## 5.2 National funding of research trials using children

79. The Nesta EdTech Innovation Testbed funded by the DfE 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. "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."<sup>43</sup>
80. Children's routine state education time should not be used to generate private for-profit products from trials in particular when children have no choice but to attend.
81. There is no consistent mechanism for schools to support families digital rights, recognise objections, or offer a route for redress to any ombudsman in education, or with whom families have some relationship or known mechanism, when required.
82. 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, "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."<sup>44</sup>
83. 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)<sup>45</sup>
84. 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%).

---

<sup>42</sup> 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>

<sup>43</sup> EdTech Innovation Testbed: FAQs for schools and colleges <https://www.nesta.org.uk/project/edtech-innovation-testbed/frequently-asked-questions/>

<sup>44</sup> 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/>)

<sup>45</sup> To obtain the perspective of parents on AI and education Nesta commissioned YouGov to undertake a survey of 1225 parents with children aged 18 and under [https://media.nesta.org.uk/documents/Future\\_of\\_AI\\_and\\_education\\_v5\\_WEB.pdf](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

85. “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)
86. 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 for domestic and for export purposes.<sup>46</sup>
87. In our 2018 commissioned poll, for *The State of Data 2018* report, many as one in four (24%) parents said they do not know if their child has been signed up to systems using personal data. When asked how often they were told if their child’s personal data will be stored or transferred to third-party organisations through a school administration software or an online learning service, only 31% of parents said they were always informed of this. 23% said they were never informed of this while 10% of parents replied, “Don’t know.”
88. 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.

### 5.3 Proposed questions on research and product trials in education

- m. Can the Department explain its policy on the involvement of children in product trials and research in educational settings and how children’s rights are considered?
- n. How is children’s right to be heard able to be exercised when it comes to participation in product or research trials?
- o. Legal guardians’ rights and duties have to be “taken into account” (Article 3(2)) and “respected” (Article 5) and all appropriate legislative and administrative measures should be taken to meet those aims. How is this consistently enabled in product trials and are there consistent standards for the sector to meet for think tank and commercial-led research projects?

## 6. Children’s social care use of big data and machine learning

89. Public policy has a state-centric, needs-based focus in public policy aimed at solving specific problems that target families for interventions and converts the parent and child into a problem to be solved. By contrast, a rights-based approach would encourage the child and guardians to be treated with their own needs at the centre of interventions, and as a holder of rights.

---

<sup>46</sup> FOI EdTech: DfE EdTech leadership group meeting transparency  
[https://www.whatdotheyknow.com/request/edtech\\_dfe\\_edtech\\_leadership\\_gro#incoming-1537342](https://www.whatdotheyknow.com/request/edtech_dfe_edtech_leadership_gro#incoming-1537342)

## 6.1 Informed consent

90. The notion of informed consent for widespread data sharing and data mining, linkage and combination with other public administrative data in such interventions is flawed and bundled together with giving agreement to accept state welfare support. As Dr Stephen Crossley, wrote in his 2018 book *Troublemakers*<sup>47</sup>:
91. *“Participants expressed unease and the amount of data that was required by central government and family’s knowledge of and consent to that data being sent.*  
*“And I really struggled with that initially, the families that were being discussed at the meetings were being discussed via a data trawl of the Government criteria” (Emma, CSM, Wesingham).*  
*“So I went back to legal and said that this question was on we do not have explicit consent from these families, to share this information with the National Troubled Families Team. What we do have is consent from the families to share information in relation to putting in place a package of support.” (Janet, CSM, Northton).*
92. If someone is profiled and targeted for interventions as a child in a Troubled Family again and again across public services, they 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.
93. The Troubled Families datasets are the core data for other child and family interventions in Local Authorities, including use in children’s social care and identifying families for intervention using predictive analytics.
94. The What Works Centre research found that, *“Children’s Services departments have substantial amounts of data available to them. This, combined with advances in computing power and algorithms, opens up the possibility of using machine learning to identify children at risk – allowing social workers to use their time to work directly with families.*
95. *However, to date it has been unclear just how effective machine learning models were at predicting which cases would escalate in future. ...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’.*
96. They did not find any evidence that the models created using machine learning techniques ‘work’ well in children’s social care. They concluded, “Given these challenges and the extent of the real world impact a recommendation from a predictive model used in practice could have on a family’s life, it is of utmost importance that we work together as a sector to ensure that these techniques are used responsibly if they are used at all.”

---

<sup>47</sup> *Troublemakers: The Construction of ‘Troubled Families’ as a Social Problem* (2018) Crossley, S, Dr ISBN 978-1447334743 (pp137-38) <https://policy.bristoluniversitypress.co.uk/troublemakers>

97. 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”, and “None of the models’ performances exceeded our pre-specified threshold for ‘success’,” 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.<sup>48</sup>
98. We believe these systems are not fit for purpose. Given growing evidence from Chicago, Philadelphia and elsewhere where such programmes were cancelled, we believe these systems do not belong in children’s social care and use should end.

## 6.2 Proposed questions on predictive algorithms in children’s social care

- p. In its oversight function for national children’s social care, can the DfE publish a list of where the local government has adopted predictive algorithms in public sector children’s social care, and from which commercial providers?
- q. What assessment has the State party made of the What Works Centre, Turing Institute and Rees Centre report on the ethics of AI in children’s social care published in January 2020<sup>49</sup>, that found “*These issues related to the safe and ethical functioning of a predictive ML (machine learning) model are magnified in high impact and safety-critical domains such as CSC, for system errors, unreliable performance, and lurking biases may have life and death consequences.*”

## 7. Understanding privacy and rights in the delivery of state education

99. Stoilova et al. (2019)<sup>50</sup> 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)

### 7.1 Children’s views on their own data and privacy

100. For the impact and perspectives on privacy as expressed by the children themselves in their own voices, may I further point the Committee to work we facilitated in workshops with young people, in 2019 and 2020 with The Warren Youth Group, Hull.

---

<sup>48</sup> 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/>

<sup>49</sup> Leslie, D., Holmes, L., Hitrova, C., and Ott, E. (2020). Ethics of machine learning in children’s social care. What Works for Children’s Social Care <https://www.turing.ac.uk/research/publications/ethics-machine-learning-childrens-social-care>

<sup>50</sup> Stoilova, M., Livingstone, S. and Nandagiri, R. (2019) Children’s data and privacy online: Growing up in a digital age. Research findings. London: London School of Economics and Political Science

1. Questions for policy makers: voices from young people from Hull and Helsinki. (length 1 minute) (2019) <https://youtu.be/u1AZH2CIRLs>
2. Our lives online and online privacy. Including big tech, and experience of exclusion from services as a result of using biometrics in schools. (length 43 minutes) (2020) <https://youtu.be/kLRRZu3L0Uk>
3. From the Warren Youth Project: "You are what you share" campaign (Hull, England) including the importance of privacy for the development of personal identity (or 'self') including gender identity and expression; and concerns over facial recognition. (length 2 minutes). <https://youtu.be/FmVZE-Y4LNE> (2019)

## 7.2 Proposed questions about digital rights in the delivery of education

101. The summer 2020 exams process in England ended in the Prime Minister blaming a 'mutant algorithm'<sup>51</sup> rather than his government taking responsibility for the outcomes that left thousands of students without GCSE and A-Level results they needed to progress to the next stage of education. There was no tool available for schools to explain how grades had been reached. Given the volume of pupil data processing teachers are asked to do from assessing progress to benchmarking schools, and lack of digital support and funding for schools in COVID-19, we are also concerned about the level of consistent capacity across the sector to meet every child's right to education in continued disruption in the pandemic.
  - r. What plans does the government have to introduce data protection, privacy, and other digital rights training into basic teacher training and continuous professional development for teachers so that they can identify error, bias and prevent discrimination in and resulting from data they are asked to create, provide to the national government, or use for their own school purposes?
  - s. How was device allocation under COVID-19 calculated, using what data, and how was it validated as accurate and meeting needs on the ground for continuing learning online at a distance, not only government numbers?
  - t. What will the government do differently in 2021 to avoid a repeat of that, and how will individual results be communicated to children, for example in the form of an individual report that explains data inputs and grade calculation, in order to meet data protection laws on algorithmic explainability?

---

<sup>51</sup> BBC (August 2020) A-levels and GCSEs: Boris Johnson blames 'mutant algorithm' for exam fiasco <https://www.bbc.co.uk/news/education-53923279>