

DUA Bill Second Reading (2024) Background Briefing for a Code of Practice in Educational Settings

<b>1. Evidence for the need for a Code of Practice on DP law in Educational Settings.....</b>	<b>2</b>
<b>2. Proposal for a Code of Practice on processing personal data in education where it concerns a child or pupil.....</b>	<b>4</b>
2.1 Definitions and Scope.....	4
2.2. The aims of a Code of Practice for Educational Settings.....	5
<b>3. Since the 2018 UK Data Protection act was adopted, what has changed?.....</b>	<b>6</b>
3.1. Automated profiling: what has changed since 2018?.....	7
3.2. National pupil processing: what has changed since 2018.....	7
3.3. Scotland and England: pupil data changes on health, sex and gender since 2018....	9
3.4. England: pupil data processing changes in edTech on mental health since 2018.....	9
3.5. Children’s Social Care: what has changed since 2018.....	10
3.6. Biometric data: what has changed since 2018.....	10
3.7. Surveillance in schools: what has changed since 2018.....	11
3.8. Pupil data security: what has changed since 2018.....	12
3.9. Large language models and Generative AI: what has changed since 2018.....	12
3.10. What other countries have done on biometrics in schools compared with the UK..	13
<b>4. Data Use and Access Bill conclusions.....</b>	<b>14</b>

## 1. Evidence for the need for a Code of Practice on DP law in Educational Settings

**Defend Digital Me is of the opinion that school children in state education in England are the least protected in domestic law and practice across Europe.** We recommend the Information Commissioner produce a Code of Practice, specific to children (up to age 18 for purposes of UK law and Convention 108) and pupils (as defined by the Education Act 1996, who may be up to age 19, or with SEND to 25) in the education sector. The duties of settings and data processors and rights appropriate to the stage of education and children's capacity, need clarity and consistency. Staff need confidence to use and access data appropriately within the law.

The new government may have staked its reputation on economic growth, but States also have obligations towards children's rights. UNCRC General Comment No. 16 (2013)<sup>1</sup> on State Obligations regarding the Impact of the Business Sector on Children's Rights, set out over a decade ago:

***"The realisation of children's rights is not an automatic consequence of economic growth and business enterprises can also negatively impact children's rights," [...]***

The Educational Setting is different from only commercial interactions or in regard to the data subjects being children. It is more complex because of the disempowered environment and its imbalance of power between the authority, the parents and child. The additional condition is parents and children's rights are interlinked, as exemplified in the Right to Education UDHR Article 26(3),

**'Parents have a prior right to choose the kind of education given to their children'.**

A Code is needed because the explicit safeguards are missing that the GDPR requires in several places but were left out of the UK 2018 drafting. **Clause 80 of the DUA Bill (automated decision-making), and the legitimate interests special condition (Part V) do not address the necessary safeguards of GDPR 23(1) for children. Furthermore removing the protections of the balancing test or Right to Object under the Legitimate Interests condition will create new risks. Clauses on additional further processing or changes to purpose limitation are inappropriately wide without child-specific safeguards for the non-consensual, disempowered environment.**

**The volume, sensitivity and intrusiveness of identifying personal data collection in educational settings only increases, while the protections are only ever reduced.**

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

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

In the UK this has not happened, so if solely automated decision making and profiling should not routinely concern a child, to respect Recital 71 of GDPR, and the CoE Principle 3.5, *"profiling of persons who cannot freely express their consent be forbidden, especially, for example, adults with incapacity and children, within the meaning of the UNCRC,"* **there must be change in policy, in practice and strong codes for effective enforcement.**

In 2017 Lord Clement-Jones said at Committee stage of the then drafting, [\[Col 1865\]](#), on Article 22 and safeguards, *"the provisions related to automated decision-taking should not be allowable in connection with children. That requires clarification."* Obligations specific to children's data, especially "solely automated decision making and profiling," and exceptions, need to be consistent, with clear safeguards-by-design where they restrict fundamental freedoms – **what does that mean for children in practice where teachers are assumed to be the rights bearers in loco-parentis?**

The need for compliance with human rights, security, health and safety among other standards proportionate to the risks of the data processing, and respecting the UK government's accessibility requirements (e.g., WCAG 2.146) should be self evident and adopted in a Code of Practice, as

<sup>1</sup> UNCRC GC no.16 (2013) <https://resourcecentre.savethechildren.net/pdf/7140.pdf/p.3> 1.1 Introduction and objectives.

recommended in the 5Rights Digital Futures Commission [Blueprint for education data governance](#).<sup>2</sup>

The Council of Europe 2022-27 Strategy on the Rights of the Child,<sup>3</sup> and UNCRC General Comment General comment No. 25 (2021)<sup>4</sup> on children's rights in the digital environment make clear that,

**Children have the right to be heard and participate in decisions affecting them, and recognises that capacity matters, *in accordance with their age and maturity.***  
In particular attention should be "*paid to empowering children in vulnerable situations, such as children with disabilities.*

It recognises in para 75, that **surveillance in educational settings should not take place without the right to object** and that teachers need training to keep up with technological developments.

UNICEF's 2017 working paper on children *Privacy, Protection of Personal Information and Reputation* said, "*it becomes evident that [children's privacy differs both in scope and application from adults' privacy.](#)*"

A code should breathe life into the [explicit recommendation](#)<sup>5</sup> of the [Working Party 29](#) to create guidance on automated decision-making with significant effects and profiling in Recital 71, such a measure 'should not concern a child' underpinned by principle of Recital 38, that children "merit specific protection." The W 29 wrote,

**"Article 40(2) (g) explicitly refers to the preparation of codes of conduct incorporating safeguards for children." (WP29 Guidelines, p.27)**

The most fundamental principle of international human rights law relating to children is that:

*In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, **the best interests of the child shall be a primary consideration.*** (UNCRC, Article 3(1)).

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

**Participation of young people themselves has not been invited in the Bill development** and the views of young people<sup>6</sup> have not been considered. However, a small sample of parent and pupil voice has been captured in the **Responsible Technology Adoption Unit public engagement work together with the DfE in 2024**. The findings backs those of our own *Survation* poll in 2018, and shows parents do not know that the DfE already holds named pupil records without their knowledge or permission and that the data is given away to be reused by hundreds of commercial companies, DWP, Home Office and police:

*"There was widespread consensus that work and data should not be used without parents' and/or pupils' explicit agreement. Parents, in particular, stressed the need for clear and comprehensive information about pupil work and data use and any potential risks relating to data security and privacy breaches."* (5.4)<sup>7</sup>

**A Code of Practice is needed to explain the law, and make it work as intended for everyone.**

<sup>2</sup> **5Rights** <https://digitalfuturescommission.org.uk/wp-content/uploads/2023/03/A-Blueprint-for-Education-Data-FINAL-Online.pdf>

<sup>3</sup> **CoE Strategy on the Rights of the Child 2022-27** <https://www.coe.int/en/web/children/strategy-for-the-rights-of-the-child>  
<https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFUI9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WxzMkZRZd37nLN1bFc2t>

<sup>4</sup> **UNCRC General Comment No.25 (2021) on the Rights of the Child in the Digital Environment**

<https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5F0vEG%2BcAAx34gC78FwvnmZXGFUI9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WxzMkZRZd37nLN1bFc2t>

<sup>5</sup> **WP29 Guidelines on Automated individual decision-making and Profiling** for the purposes of the GDPR 2016/679  
[https://defenddigitalme.org/wp-content/uploads/2017/12/20171025\\_wp251\\_enpdf.pdf](https://defenddigitalme.org/wp-content/uploads/2017/12/20171025_wp251_enpdf.pdf)

<sup>6</sup> **The Internet on our Own Terms: How children and young people deliberated about their digital rights.**(2017) Coleman, S., Pothong, K., Vallejos, E.P and Koene, A. (University of Nottingham, Horizon Digital Economy Research, 5Rights)

<sup>7</sup> **Responsible Technology Adoption Unit: Research on public attitudes towards the use of AI in education (2024)**  
<https://www.gov.uk/government/publications/research-on-parent-and-pupil-attitudes-towards-the-use-of-ai-in-education/research-on-public-attitudes-towards-the-use-of-ai-in-education>

## 2. Proposal for a Code of Practice on processing personal data in education where it concerns a child or pupil

### Insert the following new Clause—

“Code on processing personal data in education where it concerns a child or pupil

- (1) The Commissioner must consult on, prepare and publish a Code of Practice on standards to be followed in relation to the collection, processing, publication and other dissemination of personal data concerning children and pupils in connection with the provision of education services in the UK, within the meaning of the Education Act 1996, the Education (Scotland) Act 1996, and The Education and Libraries (Northern Ireland) Order 1986; and appropriate to children’s capacity and stage of education.
- 2) For the purposes of subsection (1), “the rights of data subjects” must include—
  - (a) measures related to responsibilities of the controller, data protection by design and by default; and security of processing;
  - (b) safeguards and suitable measures with regard to automated decision-making, including profiling and restrictions;;
  - (c) the rights of data subjects including to object to or restrict the processing of their personal data collected during their education, including any exemptions for research purpose ;  
and
  - (d) matters related to the understanding and exercising of rights relating to personal data and the provision of education services.”

### 2.1 Definitions and Scope

- Education is devolved. [Compulsory education ages](#) are different and the issue of being in a setting where everyone is treated as a child but some are over 18 does not arise elsewhere. This Code could be extended to devolved nations within the appropriate legislation in addition to the Education Act 1996 for England and Wales or limited in scope.
- For example, in the Education Act 1996, “pupil” means a person for whom education is being provided at a school, other than—
  - (a) a person who has attained the age of 19 for whom further education is being provided, or
  - (b) a person for whom part-time education suitable to the requirements of persons of any age over compulsory school age is being provided.

A Code does not hinder any regional developments in progress. It would however be appropriate if child rights as regards data were shaped to apply across the UK consistently.

Within the meaning of “pupil” ICO can recommend and consider capacity appropriate standards not only on age, but in the best interests of every pupil, within the meaning of [the 1996 Education Act](#)<sup>8</sup>, (England and Wales) the Education (Scotland) Act 1996, and The Education and Libraries (Northern Ireland) Order 1986.

There are also pupils in education who are no longer children under 18 for whom parental responsibilities can continue up to age 25 for learners with [SEND and an EHC plan in education](#), but for whom data protection law generally, makes no provision beyond age 18. While [SEND legislation](#) takes account of this, a data Bill without mention of children’s capacity not age, does not.

<sup>8</sup> The Education Act (1996) meaning of “pupil” <http://www.legislation.gov.uk/ukpga/1996/56/section/3>

## 2.2. The aims of a Code of Practice for Educational Settings

1. Adherence to a code creates a mechanism for
  - a. controllers and processors to “*demonstrate compliance with the legislation or approved certification mechanisms.*” [GDPR Articles 24(3)]
  - b. providers’ confidence in consistent and clear standards, good for the edTech sector
  - c. children, parents, school staff and systems administrators to build trust in safe, fair and transparent practice, so their rights are freely met by design and default
2. Schools give children’s personal data to many commercial companies during a child’s education, not based on consent, Article 6(1)(a) or 8(1), but assumed, “*for the performance of a task carried out in the public interest.*” A code should clarify any boundaries of this lawful basis for commercial purposes, where it is an obligation on parents to provide the data, and what this means for the child on reaching maturity or after leaving the educational setting.
3. A Code should help companies understand “*data protection by design and default*” in practice, and [child] appropriate ‘significant legal effect’ (Baroness Ludford, Second Reading in the 2017 Act debate, [Col 144-5](#)). The edges of ‘public interest’ in data transfers to a third country, and how 9(2)(g) (special categories of data), affects children in schools.
4. A Code should support children and families, understand the effect of the responsibilities of controllers and processors, for the execution or limitations of their own rights.
5. The Article 29 WP further recommends, “*Because children represent a more vulnerable group of society, organisations should, in general, refrain from profiling them for marketing purposes.*” How should this be understood for software platforms that profile users’ meta-data to share with third parties, or commercial apps signed-up-for in schools that offer adverts in-use, or bait and switch premium models of selling to pupils leaving school?<sup>9</sup>
6. Setting out child appropriate safeguards is necessary under GDPR Articles 13(2)(f), and 21-23 for exemptions. The current Act fails to set out required safeguards for children.
7. Definitions of “*appropriate technical and organisational measures*” and what is expected to be “*appropriate to the risk*” for children under Recital 38 (children merit special protection) and UNCRC principles are needed. Small businesses and schools need information on acceptable and necessary levels of “*pseudonymisation, encryption, and on transmission*”.
8. Joint-controllers treat the same data differently. Schools need guidance on compliance where
  - i) processing data under instructions from the controller(s) may differ from their own need and
  - ii) there is a potential conflict in the best interests and restriction of the fundamental freedoms of the child, for example in regard to exports of school census data, for commercial re-use.
9. Further important rights the amendment addresses include with reference to GDPR Article 40: (h) the measures and procedures referred to in [Articles 24\(3\)](#) (responsibility of the controller) and [Article 25](#) (especially “*by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons*”), and retention periods, and measures to ensure security of processing ([Article 32](#)); (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; and (j) the transfer of personal data to third countries or international organisations.

---

<sup>9</sup> **Class Dojo poses Data protection Concerns for Parents (2017)** Williamson, B. and Rutherford, A.  
<http://blogs.lse.ac.uk/parenting4digitalfuture/2017/01/04/classdojo-poses-data-protection-concerns-for-parents/>

For common case studies of profiling in education in England see [our submission to WP29](#).<sup>10</sup>

### 3. Since the 2018 UK Data Protection act was adopted, what has changed?

In 2017, in the drafting of the UK Data Protection Act 2018, peers debated the introduction of a Code of Practice for educational settings in [amendment 117](#) in the name of the Earl of Clancarty.

Nothing was done.

**In the November 2023 House of Lords short debate on Educational Technology**<sup>11</sup> it was suggested that there are alternative visions. One dystopian, with “all the problems of data privacy and privatisation”. Alternatively, a utopian vision of technology as “a co-pilot to teachers”.

This briefing sets out to present neither, but simply show the as-is state of practice across the landscape of educational data processing for children in state educational settings today as it has developed since 2018 when the UK Data Protection Act came into effect. A selection of case studies demonstrate the failure of schools to take data protection from legislation into practice and to make the case for why a Code of Practice is needed to give schools, parents and learners the clarity, confidence and consistency needed to raise standards across the sector. It cannot wait longer.

The introduction of many common technology tools, apps and platforms into the school setting without procurement safeguards, means the introduction of hundreds, often thousands, of strangers who influence a child’s life through interactions with companies and their affiliates in the digital world. There have been no “lessons learned” or changes made even since the case involving **a convicted paedophile and former teacher who was identified as running a major UK education website**.<sup>12</sup>

But the enormous regular collection of pupil data on a named basis retained forever by the State must not be forgotten in any eagerness to rein in the practices of Big Tech<sup>13</sup> or EdTech. Governments repeatedly say they want to collect more data, including a register of those receiving education otherwise than state settings. Parents who do not trust the state with their child’s education are not inclined to trust a Department for Education where the data practices are in breach of the law.

Our aim is for all education data processing across the public sector to be safe, fair and transparent.

**This Bill brings new risks for children where the additional use and access of identifying data collected for service provision or administrative purposes, is not intended for ‘research purposes’ or reuse at all:**

- **Risks of contextual collapse when used operationally;**
- **No way to know when errors are made;**
- **No routes for remedy or redress if you are wrongly caught up in any intervention.**

Data is controlled, not owned, and that carries obligations to communicate to those in the dataset. Around 15 million people of the 23 million in the National Pupil Database (NPD) have already left school and that number grows each year. When will the DfE inform them, including most of the 200 MPs aged under 50 today, whose own records may be included in the data reused and given away, or anyone whose children and grandchildren are in the NPD today?

These case studies demonstrate a wide range of lack of protections in place across the full spectrum of applications from learning platforms and apps, to school administrative systems from cashless payment systems to behavioural monitoring online and in the classroom. These data processing matters affect children of all age ranges, across all school types, from preschool to University, and at local to national levels. A Code of Practice is needed to explain the law and make it work as intended.

<sup>10</sup> **Submission on the WP29 guidance on automated processing and children - sample case studies in England pp 3-6**  
[http://defenddigitalme.org/wp-content/uploads/2017/12/DDM\\_Response-to-Working-Party-29-Guidelines-on-Automated-individual-Decision-making-and-Profiling-for-purposes-of-Regulation-2016\\_679\\_v1.2-2.pdf](http://defenddigitalme.org/wp-content/uploads/2017/12/DDM_Response-to-Working-Party-29-Guidelines-on-Automated-individual-Decision-making-and-Profiling-for-purposes-of-Regulation-2016_679_v1.2-2.pdf)

<sup>11</sup> **House of Lords short debate on Educational Technology** Vol. 834  
<https://hansard.parliament.uk/lords/2023-11-23/debates/0588AF21-816D-4556-9D84-93D9A2385A07/EducationalTechnology>

<sup>12</sup> **Paedophile ran teaching website (2010)** BBC <http://news.bbc.co.uk/1/hi/8462650.stm>

<sup>13</sup> **Letter of the Chair of the Article 29 Working Party to Microsoft** (15.02.2017)  
[http://ec.europa.eu/newsroom/document.cfm?doc\\_id=42947](http://ec.europa.eu/newsroom/document.cfm?doc_id=42947)



### 3.1. Automated profiling: what has changed since 2018?

In the 2020 summer examinations under COVID, almost 40% of students received grades lower than they had anticipated,<sup>14</sup> sparking public outcry and legal action. **Thousands of children were graded by algorithm and we saw furious student protests at the DfE.**<sup>15</sup> Not only were children harmed in ways they could not influence, they had **no agency or routes for remedy or redress** once it happened. That has not changed.

This presents an example of a key accountability challenge standing in the way of responsible use of algorithms, in particular where more use is foreseen with sole decision making with significant effect. A challenge the public sector needs to solve and that must start with **duties on explainability.**<sup>16</sup>

### 3.2. National pupil processing: what has changed since 2018

**A 2020 ICO audit of national pupil data processing at the Department for Education, affecting over 21 million people** (children and adults aged under 48, having left state education):

*“found data protection was not being prioritised and this had severely impacted the DfE’s ability to comply with the UK’s data protection laws. A total of 139 recommendations for improvement were found, with over 60% classified as urgent or high priority.”<sup>17</sup>*

*“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.”*

In 2020, the Sunday Times reported **an approved third-party user of the Learner Records Service**, Trustopia, with access to the LRS database searches on 22,000, **was using it to enable gambling companies to check whether people opening new accounts were over 18.**<sup>18</sup>

*“Since using GBG UK Education Data Set within our ID3global product, a major gambling operator saw a 15% uplift to a 2+2 on customer refers, while a digital currency wallet business saw a 9% uplift.”*

**Nearly 3 years (34 months)<sup>19</sup> after the Learner Records Service breach was exposed in the press on January 20, 2020, the ICO announced it had reprimanded the DfE** over the incident. According to the ICO<sup>20</sup>, *“This was a serious breach of the law worthy of a £10m penalty”* and yet neither the DfE in the public sector nor the data processor (where the actions were arguably unlawful) were fined. **The commercial company directors<sup>21</sup> carry on businesses elsewhere as usual.**

Once pupils’ data have left school systems and are sent to the DfE in the termly school census, the

<sup>14</sup> **LSE (2020) “F\*\*k the algorithm”?: What the world can learn from the UK’s A-level grading fiasco**  
<https://blogs.lse.ac.uk/impactofsocialsciences/2020/08/26/fk-the-algorithm-what-the-world-can-learn-from-the-uks-a-level-grading-fiasco/>

<sup>15</sup> **BBC (2020) A-levels and GCSEs: Boris Johnson blames 'mutant algorithm' for exam fiasco**  
<https://www.bbc.co.uk/news/education-53923279>

<sup>16</sup> **Restoring trust in awarding exam grades: the case for a Personal Exam Grade Explainer** (2021) Defend Digital Me  
<https://defenddigitalme.org/2021/12/04/restoring-trust-in-awarding-exam-grades-the-case-for-a-personal-exam-grade-explainer/>

<sup>17</sup> **ICO Audit of the DfE in 2020 Summary (the full findings have never been published to date)**  
[https://web.archive.org/web/20201007192642/https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1\\_0.pdf](https://web.archive.org/web/20201007192642/https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf)  
ICO statement

<https://web.archive.org/web/20201007192747/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>18</sup> **GBG plc on how their gambling onboarding rates increased using the learners dataset**  
<https://web.archive.org/web/20191226143014/https://www.gbGPLC.com/newsroom/the-exclusive-data-that-boosts-millennials-onboarding-rates/>

<sup>19</sup> **The Learner Records Service Data Breach and ICO audit: a connected chronology (Defend Digital Me)**  
(Defend Digital Me) <https://defenddigitalme.org/the-learner-records-service-data-breach-and-ico-audit-a-connected-chronology/>

<sup>20</sup> **ICO statement on the LRS Data Breach 2018-20**  
<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/11/department-for-education-warned-after-gambling-companies-benefit-from-learning-records-database/#>

<sup>21</sup> **Trustopia directors in 2020 at the time of the breach reported in the Sunday Times**  
<https://web.archive.org/web/20200120071830/http://webcache.googleusercontent.com/search?q=cache:i4b7HMv7J9kJ:https://www.trustopia.com/trustopia-leadership-team>

**DfE cannot tell schools or the learners or their families in which of the thousands of distributions they have given away a child's named or identifiable, sensitive data** in any record from the National Pupil Database,<sup>22</sup> now holding the personal confidential data of over 23 million people without their knowledge or consent. In [answer to PQ 109113](#) the DfE do not know how many children's identifying data they have given away since 2012 because, "**The Department does not maintain records of the number of children included in historic data extracts.**"<sup>23</sup>

Since 2018 the DfE expanded the school census individual named pupil data collected to broaden the SEN type codes, updated to include **Down Syndrome**.<sup>24</sup> New items for **reasons for transfer including pregnancy, and young offender** were added to the school census AP module in 2019. The **Service Child** indicator for children from military families increased from once a year to being collected each term.<sup>25</sup> And of course, the COVID reason for absence was added, and withdrawn. A new ethnicity code was added in 2021 of **White Northern Irish**. **Highly sensitive peer-on-peer categories of abuse**<sup>26</sup> were added in 2021 to the Children in Need Census. A **young carer** label was added in 2022. A **Gender Identity** field was approved by DfE for local use in 2023.<sup>27</sup>

The collection of pupil nationality and country of birth begun in 2016 were dropped by the department in 2018, after it was demonstrated the aims of the new data collection included furthering the Hostile Environment. **Monthly handovers of pupil data continue, and to date the Home Office has sought matched details of nearly 7.2K individuals and the DfE has given them matched data from education records, for over one thousand eight hundred.**<sup>28</sup>

In 2018, the DWP made a request "involving 185 child identities to be checked against the national pupil database. In 2019 the DWP began requesting huge volumes of data from national pupil records."<sup>29</sup> Later that year a data sharing agreement was set up for the DWP to make requests from the DfE to access education records to match for Universal Credit fraud detection.<sup>30</sup>

Two new national primary school pupil testing programmes began in England since 2018. **The Multiplications Times Tables Checks** collect pupil level identifying data since 2019, with personal details to be analysed by "psychometricians".<sup>31</sup> **The Reception Baseline Test began in 2021.**<sup>32</sup> The DfE began collecting school attendance data daily on a named basis from every on-roll child.<sup>33</sup>

**In none of the school census data expansions or new national primary tests were any of the changes effectively communicated to parents with their rights. None offered a route to exercise a right to object, as required in data processing under the public task. There is still a completely inadequate Subject Access Request process and no way to know where your own data have gone beyond a generic distribution list of all third party data sharing from the Department for Education.**

---

<sup>22</sup> <https://www.find-npd-data.education.gov.uk/categories>

<sup>23</sup> **UIN 109113: "The Department does not maintain records of the number of children included in historic data extracts."**  
<http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-10-23/109113/>

<sup>24</sup> **Young carer census label added 2022**

[https://defenddigitalme.org/wp-content/uploads/2022/11/CBDS\\_RFC\\_1201\\_-\\_School\\_census\\_changes.pdf](https://defenddigitalme.org/wp-content/uploads/2022/11/CBDS_RFC_1201_-_School_census_changes.pdf)

<sup>25</sup> **The Department for Education School Census Guide 2018 - 2019**

[https://assets.publishing.service.gov.uk/media/5c66975be5274a72b55d589a/2018\\_to\\_2019\\_School\\_Census\\_Guide\\_V1\\_7.pdf](https://assets.publishing.service.gov.uk/media/5c66975be5274a72b55d589a/2018_to_2019_School_Census_Guide_V1_7.pdf)

<sup>26</sup> **CIN 2021 Categories of abuse added to the national individual level data collection**

[https://assets.publishing.service.gov.uk/media/60743257d3bf7f401659fd90/CIN\\_Additional\\_guide\\_on\\_the\\_factors\\_identified\\_at\\_the\\_end\\_of\\_assessment.pdf](https://assets.publishing.service.gov.uk/media/60743257d3bf7f401659fd90/CIN_Additional_guide_on_the_factors_identified_at_the_end_of_assessment.pdf)

<sup>27</sup> **Gender identity field added to school information managements systems at DfE for local use (2023)**

[https://assets.publishing.service.gov.uk/media/642bf367f6e62000f17dbc7/CBDS\\_RFC\\_1233\\_-\\_Sex\\_and\\_Gender\\_Identity.pdf](https://assets.publishing.service.gov.uk/media/642bf367f6e62000f17dbc7/CBDS_RFC_1233_-_Sex_and_Gender_Identity.pdf)

<sup>28</sup> **External data shares between July 2024-July 2015** <https://www.gov.uk/government/publications/dfe-external-data-shares>

<sup>29</sup> **DfE Data Sharing Approval Panel (DSAP) DWP Request No:DS00259 Request (DR) reference No: DR180731.01**

[https://www.whatdotheyknow.com/request/the\\_pupil\\_parent\\_matched\\_dataset/response/2139981/attach/5/NPD%20Request%20DWP%20Data%20Schedule%20REDACTED.pdf](https://www.whatdotheyknow.com/request/the_pupil_parent_matched_dataset/response/2139981/attach/5/NPD%20Request%20DWP%20Data%20Schedule%20REDACTED.pdf)

<sup>30</sup> **Schools Week (2024) Revealed: Secret deal to let benefit fraud squad snoop on pupil data**

<https://schoolsweek.co.uk/revealed-secret-deal-to-let-benefit-fraud-squad-snoop-on-pupil-data>

<sup>31</sup> **Multiplication Tables Check (MTC) begun (2019)** Defend Digital Me

<https://defenddigitalme.org/2019/05/10/the-multiplication-tables-check-mtc/>

<sup>32</sup> **Reception Baseline Test begun (2021)**

<https://defenddigitalme.org/2020/06/25/baseline-beaten-back-to-2021-time-for-change-in-the-accountability-system/>

<sup>33</sup> **Challenging the Department for Education on excessive pupil data collection (2022-24)** DDM

<https://defenddigitalme.org/2022/09/16/news-challenging-the-department-for-education-on-excessive-pupil-data-collection/>



In Higher Education across the UK, ever more equality data has been collected and **retained on a named basis** via JISC<sup>34</sup> from students including sexual orientation, disabilities and religion. As of February 2023, the DfE held the self-declared **sexual orientation of 3,213,683 and the religious affiliation of 3,572,489 people on a named basis in the National Pupil Database. In a sample of 30 UK Universities only one has carried out any Data Protection Impact Assessment.** It found if the data were breached, risk of harm and **threat to life**.<sup>35</sup> Students are not informed of this.

### 3.3. Scotland and England: pupil data changes on health, sex and gender since 2018

In 2021-22 the **Health and Wellbeing Census** took place in schools across **Scottish local authorities,\* retaining the children's unique school identifier number.** Sixteen of 32 withdrew from the process, 12 due to concerns. It caused outrage and objection in some parents when it was discovered that **the survey asked about detailed sexual behaviours and abuse.** Or as the **Office for National Statistics Regulation** wrote,

“There has been significant media coverage and several freedom of information requests to the Scottish Government regarding **the appropriateness of the question on sexual experience in the Health and Wellbeing Census** that is asked.”<sup>36</sup>

The OSR recommended that the census be reviewed including concerns with collection practices and what people were told and, “the outcomes of this review should be made publicly available”. **That has not happened. It continues to undermine the trustworthiness of future Health and Wellbeing Censuses in Scotland and some parents are considering withdrawing children from school.**

In England, over 100 local council **schools' admissions forms in England ask for 3 year-old's gender identity.**<sup>37</sup> There is no consultation duty or oversight of any new mass pupil data collections.

### 3.4. England: pupil data processing changes on mental health since 2018

**Mental health and wellbeing apps: Lack of effective regulation:**

Steer Education Ltd **claims to have tracked and supported at least 150,000 students in over 250 primary and secondary schools across the state and independent sector. These include leading MATs, specialist schools and elite sports academies.**<sup>38</sup> Tracking the “steering biases which are **developing in the mind of a student**”.

Defend Digital Me supported parents in making a complaint to the regulator including that there was no transparent way that children, staff or parents can independently validate any company health claims, and it is excessive for a school to, “curate a unique 10 year record of a child's social-emotional development, monitoring their wellbeing through adolescence.” **They were concerned a company could influence their child's mental health or make some sort of assessment about it, without parents or professionals being able to understand it, and that the data handed over included highly sensitive information** such as ‘recently bereaved’, “with a welfare plan”, “heavily committed”, “gifted”, and “nationality”.

In February 2020, defenddigitalme was told the Office of the Information Commissioner had:

*"made enquiries with STEER, and....found that it is likely that STEER and the schools using their services are in contravention of the UK General Data Protection Regulations (UK GDPR) or Data Protection Act 2018 (DPA18). I can confirm that this finding means that I*

<sup>34</sup> **UIN HL4026 Equality monitoring data**

<https://questions-statements.parliament.uk/written-questions/detail/2024-04-23/HL4026/>

<sup>35</sup> **Equality monitoring data data impact assessment found threat to life:** Access the original FOI requests at Defend Digital Me <https://defenddigitalme.org/2023/04/02/does-your-national-school-record-reveal-your-sexual-orientation/>

<sup>36</sup> **OSR (2022) Director General for Regulation, Office for Statistics Regulation Health and Wellbeing Census in Scotland**

<https://osr.statisticsauthority.gov.uk/correspondence/ed-humpherson-to-alastair-mcalpine-health-and-wellbeing-census-in-scotland/>

<sup>37</sup> **Fury as councils ask parents for 3-year-old's gender ID in school admissions** (2024) Daily Mail

<https://www.dailymail.co.uk/news/article-14066125/Fury-councils-ask-parents-gender-ID-used-three-year-old-child-school-application-form.html>

<sup>38</sup> **STEER** <https://steer.education/summary-findings-young-peoples-mental-health-in-the-uk-steer-report-feb-2022/>

*partially uphold the concerns you raised around Article 5(1)(a), Article 5(1)(b), Article 9, and Article 35 of the UK GDPR.”*

**There was no enforcement action published. Despite all their claims around mental health<sup>39</sup>, they remain unregulated in education, rather as would be in the health sector.** They pass the tool on to the children when they leave school, aged 16. They are unregulated by the clinical healthcare market. The company has since expanded to now sell schools ‘safeguarding’ solutions<sup>40</sup>.

**The “wellness” industry is now all over education, with product marketing and trials for things like wearables in schools, often with harmful not beneficial outcomes and effects.** Researchers even found, “healthy lifestyle technology may have negative motivational consequences for teens”.<sup>41</sup>

**Wellness is not regulated** and is a marketing term, and avoids health regulation. What the government plans are for the forthcoming, “Children’s Wellbeing Bill”<sup>42</sup> remain to be seen.

### 3.5. Children’s Social Care: what has changed since 2018

**Predictive algorithms have been marketed hard at strapped-for-cash children’s services.**

**One of the schemes that has attracted most controversy** – Hackney council’s Early Help Profiling System (EHPS), commissioned from private provider Xantura – **was dropped after it did not “realise the expected benefits”**.<sup>43</sup> “There are widespread conditions of poor data quality and questionable data collection and recording practices and amplifying, historical patterns of systemic bias and discrimination.<sup>44</sup> and **according to a 2020 Turing Institute report**, the [machine learning] **“models will potentially contain dangerous blind-spots.”**

In England, Michael Sanders, Chief Executive of the What Works for **Children’s Social Care** in September 2020, as regards predictive machine learning used in children’s social care, said,

*“now is the time to stop and think, not ‘move fast and break things’. “With the global coronavirus pandemic, everything has been changed, all our data scrambled to the point of uselessness in any case.”<sup>45</sup>*

### 3.6. Biometric data: what has changed since 2018

In 2021 schools in Scotland across North Ayrshire began using **facial recognition<sup>46</sup> for pupils buying lunches** in the school canteen<sup>47</sup> and the ICO had to step in as an emergency reaction.<sup>48</sup> In the Scottish Parliament, the MSP for North East Fife Willie Rennie, asked what the Scottish government position is on facial recognition in schools. Then First Minister, Nicola Sturgeon responded that she felt **the technologies do not appear to be proportionate or necessary.**<sup>49</sup>

<sup>39</sup> <https://steer.education/summary-findings-young-peoples-mental-health-in-the-uk-steer-report-feb-2022/>

<sup>40</sup> **Defend Digital Me (2020) See 3.10.4 Socio-emotional mental health tracking | Case study STEER AS** Tracking in our report <https://defenddigitalme.org/research/the-state-of-data-2020/report/> and <https://steer.education/safeguarding/>

<sup>41</sup> Kerner and Goodyear (2017) **The Motivational Impact of Wearable Healthy Lifestyle Technologies: A Self-determination Perspective on Fitbits With Adolescents** American Journal of Health Education\_Volume 48, 2017 - Issue 5: Health Education and Health Promotion in College Settings - Part II | <https://www.tandfonline.com/doi/full/10.1080/19325037.2017.1343161>

<sup>42</sup> **Children’s Wellbeing Bill announced in the King’s Speech 2024**

<https://educationhub.blog.gov.uk/2024/07/18/the-kings-speech-2024-what-does-it-mean-for-education>

<sup>43</sup> Using algorithms in children’s social care: experts call for better understanding of risks and benefits (2019)

<https://www.communitycare.co.uk/2019/11/15/using-algorithms-childrens-social-care-experts-call-better-understanding-risks-benefits/>

<sup>44</sup> **Ethics review of machine learning in children’s social care.** Leslie, D., Holmes, L., Hitrova, C., & Ott, E. (2020). .

<https://doi.org/10.5281/zenodo.3676569>

<sup>45</sup> **Machine Learning; Now is a time to stop and think (Children’s Social Care)** Sanders, M. (2020)

<https://whatworks-csc.org.uk/blog/machine-learning-now-is-a-time-to-stop-and-think/>

<sup>46</sup> **Parliamentary briefing (2021) Facial Recognition in Schools**

<https://lordslibrary.parliament.uk/facial-recognition-technology-in-schools/>

<sup>47</sup> **FT (2021) Facial Recognition Cameras arrive in UK School Canteens**

<https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9>

<sup>48</sup> **ICO to step in after schools use facial recognition to speed up lunch queue** (2021)

<https://www.theguardian.com/education/2021/oct/18/privacy-fears-as-schools-use-facial-recognition-to-speed-up-lunch-queue-ayrshire-technology-payments-uk>

<sup>49</sup> **Facial Recognition Technology (Schools) – question in the Scottish Parliament on 28 October 2021** (They Work For You). <https://www.theyworkforyou.com/sp/?id=2021-10-28.23.0&s=speaker%3A25111>

**After Defend Digital Me national research in 2022<sup>50</sup>, we estimate there is likely unlawful adoption or use of fingerprint and facial recognition biometric systems in around 75% of UK secondary schools including discrimination where “students who qualify for FSM need to be signed up to the biometric system in order to continue to receive their lunch”.<sup>51</sup>**

Survation polled 1,004 parents of children aged 5-18 in state education in England on behalf of defenddigitalme in February 2018. **Over a third (38%) of those who said their child’s school uses biometric technology, said they were not offered a choice of whether to use this system or not, despite the law that requires parental consent, the Protection of Freedoms Act 2012.**

**Biometrics are being used to infer mood and emotions.** ViewSonic introduced a product using “AI algorithms” it claimed could monitor, “*every student’s facial expression for real-time tracking*” and identify one of five moods.<sup>52</sup>

**On November 4, 2021 the House of Lords held a short debate**, led by the question from Lord Clement-Jones, to ask Her Majesty’s Government what assessment they have made of the use of **facial and other biometric recognition technologies in schools.**<sup>53</sup>

Baroness Falkner said,<sup>54</sup>

“what is needed is to **strengthen existing protections for this AI-driven world that offer clear legal remedies for people wronged** that go beyond data privacy and allow us to **know as a matter of right who holds what data on us, how it is being used and, importantly, how much is being transferred**, at what profit, to others without our knowledge”.

But nothing has changed. Use and access simply keep expanding, parents and children feel helpless.

### 3.7. Surveillance in schools: what has changed since 2018

Cameras and voice recording always on in the classroom: A technical college in Birmingham for 14- to 19-year-olds, became the first school in the country to install **always-on, 360-degree cameras with high spec audio recording in all of its 28 classrooms.**<sup>55</sup> This week parents of infants at a primary school asked Defend Digital Me to write on their behalf to the Information Commissioner because their school has installed the same recording systems, without consultation or a risk assessment prior to starting, and has told parents they cannot object and that consent is not needed.

**“Safeguarding in Schools” monitoring tech:** Since 2018, three leading UK school safeguarding companies have been bought out affecting thousands of students’ data transfers. In 2021 eSafe was bought by Smoothwall which in turn became part of Qoria<sup>56</sup> owned by Australian firm Family Zone.<sup>57</sup>

**SafetyTech company staff where the ‘safeguarding in schools’ is run through a managed service, or some cloud based providers, are able to see children’s nudes and highly sensitive data sent to the company from children’s devices, Defend Digital Me had confirmed from three of the leading “safetyTech” firms in England** in January 2024 and there is no accountability at the Department for Education to put any regulations into practice or law to prevent misuse, where one team is responsible for technical standards and another for schools guidance.<sup>58</sup>

<sup>50</sup> The **State of Biometrics report (2022)** King, P. and Persson, J. <https://defenddigitalme.org/research/state-biometrics-2022/>

<sup>51</sup> **Sample school notice on FSM and fingerprint systems**

<https://buxtonschool.s3.amazonaws.com/uploads/document/Biometrics-Policy.pdf?t=1731623500>

<sup>52</sup> **ViewSonic (2020) “Detects 5 emotions through expression recognition: Happy / Sad / Upset / Amazed / Attentive”**

[https://www.viewsonic.com/vsAssetFile/global/img/vertical\\_site/resources/upload/files/MVB%20Sens%20Brochure\\_Final\\_0223.pdf](https://www.viewsonic.com/vsAssetFile/global/img/vertical_site/resources/upload/files/MVB%20Sens%20Brochure_Final_0223.pdf)

<sup>53</sup> **House of Lords debate: Biometric Recognition Technologies in Schools.** Volume 815 on Thursday 4 November (2021)

<https://hansard.parliament.uk/lords/2021-11-04/debates/26FB2DF4-8D5A-456B-AFDA-73501D1CCBD3/BiometricRecognitionTechnologiesInSchools>

<sup>54</sup> **Baroness Falkner of Margravine, Biometric Recognition Technologies in Schools (2021)**

<https://hansard.parliament.uk/lords/2021-11-04/debates/26FB2DF4-8D5A-456B-AFDA-73501D1CCBD3/BiometricRecognitionTechnologiesInSchools#contribution-82BDCBBF-E855-499E-93C2-B9381A8CBCC5>

<sup>55</sup> **Schools Week (2018) UTC becomes first school with cameras in every classroom** – costing reportedly £4,500 per room

<https://schoolsweek.co.uk/utc-becomes-first-school-with-cameras-in-every-classroom/>

<sup>56</sup> **Leeds-based Smoothwall acquired by Australian company Family Zone Cyber Safety Limited for £75.5m (2021)**

<https://www.yorkshirepost.co.uk/business/smoothwall-has-been-acquired-by-family-zone-cyber-safety-limited-for-ps755m-3336374>

<sup>57</sup> **Qoria** <https://www.listcorp.com/asx/qor/qoria-limited/news/family-zone-completes-acquisition-of-smoothwall-2577193.html>

<sup>58</sup> **DfE guidance: Meeting digital and technology standards in schools and colleges**

### 3.8. Pupil data security: what has changed since 2018

A 2023 government-commissioned [survey](#) found **education institutions were more likely to have identified cyber breaches or attacks in the past year than the average UK business**. The survey of 241 primaries and 217 secondaries by market research firm Ipsos found **41 per cent of primaries and 63 per cent of secondaries had identified breaches or attacks in the past 12 months**. This compared with 32 per cent of 2,263 surveyed businesses.<sup>59</sup>

US-based education platform Edmodo [confirmed](#) 77 million account details were stolen – **more than 2 million of them in the UK** – across 550,000 schools worldwide. It was subsequently bought out by Chinese owned firm NetDragon, in 2018.

In February this year, some **parents logging on to Class Charts, used by more than 180,000 teachers, were reportedly shown data relating to other people's children**, in an unknown number of schools. IT professionals agreed it was a breach<sup>60</sup>, but the company did not. As **part of a prior investigation the ICO revealed that the company did not use AI despite many of its website claims about it being “driven by Artificial Intelligence” as its unique selling point**. “NQTs, supply & cover teachers will love how our AI engine automatically suggests seating plans optimised for learning & behaviour,” they claimed. The product was mis-described for years to schools and is still widely used in the education sector today. The ICO never published its findings.

Most recently Schools Week<sup>61</sup> reported that the latest count of total **hacked pupil records at Capita had risen to more than 50k, and included names, dates of birth, unique pupil number, type of test taken and the schools' DfE number**. Everything needed for identity theft.

In Northern Ireland, due to security practices that permitted a failure of human error, an email issued on 1 August 2024 shared a spreadsheet in error of **Special Educational Needs (SEN), names, email address and titles of 407 individuals** who had registered an interest in attending End-to End Review of SEN events across NI.<sup>62</sup>

### 3.9. Large language models and Generative AI: what has changed since 2018

Everything. **ChatGPT and large language models have crash landed into the education sector as stand alone products, and also been integrated at pace into hundreds of edTech apps**.

**There is widespread ignorance of company policies on children's use**. To use ChatGPT a child must be at least 13 years old and if under 18 must have a parent or legal guardian's permission.<sup>63</sup> Since valid consent for a learner, especially a child, in a non-consensual disempowered setting is almost impossible to achieve where it is made routine for any classroom or homework activity, the **data processing basis of 'consent' is not valid for schools to use or request from parents**.

**As Baroness Harding reported in November 2023, research<sup>64</sup> of 1,000 secondary school students found 67% of them already used [...] ChatGPT—six months after it launched.**<sup>65</sup>

<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges>

<sup>59</sup> **DSIT (2023) Cyber security breaches survey 2023: education institutions**

<https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex>

<sup>60</sup> **Classcharts (2024)** <https://www.edugeek.net/forums/mis-systems/236405-classcharts-gdpr-security-issue.html>

<sup>61</sup> **Capita Hack of 50K school children (2024)**

<https://schoolsweek.co.uk/hacked-pupil-records-at-capita-rise-to-more-than-50k/>

<sup>62</sup> **Northern Ireland Department of Education statement on data breach**

<https://www.education-ni.gov.uk/news/department-education-statement-data-breach>

<sup>63</sup> **OpenAI terms of service** <https://openai.com/policies/terms-of-use/>

<sup>64</sup> **A poll on AI in education (2023) commissioned by RM Technology and conducted by Perspectus Global in June 2023** <https://www.rm.com/news/2023/artificial-intelligence-in-education>

<sup>65</sup> **Reference made to “Statistics from an RM Technology research pamphlet” Col. 116GC**

<https://hansard.parliament.uk/lords/2023-11-23/debates/0588AF21-816D-4556-9D84-93D9A2385A07/EducationalTechnology#contribution-24F29E87-3F45-498D-A86B-4486792719CE>

This year, HEPI found that more than a third of students who have used generative AI (35%) do not know how often it produces made-up facts, statistics or citations ('hallucinations').<sup>66</sup> Business Insider reports, "OpenAI's creators have said that [AI could surpass human expertise in most areas within the next 10 years](#) and some fear the technology [poses an existential risk](#)." Yet despite lawsuits claiming data theft in the U.S. there has been no regulatory action vs OpenAI in the UK:

*"A lawsuit claims **OpenAI stole 'massive amounts of personal data,' including medical records and information about children, to train ChatGPT.**" (Business Insider).*

### 3.10. What other countries have done on biometrics in schools compared with the UK

In **France** a court found the use of facial recognition in high schools unlawful. The French data protection authority, the CNIL, ordered high schools in Nice and Marseille to end their facial-recognition programs. The controller had failed to demonstrate that its objectives could not have been achieved by other, less intrusive means.<sup>67</sup>

In 2020 a school in **Poland** was fined and banned from using biometric fingerprint technology in the school canteen. The Data Protection Authority found the introduction of fingerprints created an unequal treatment of students, as it favoured students who used biometric identification. The authority considered the use of biometric data, "significantly disproportionate".

**Sweden** issued its first fine under GDPR to a school in its case, and found consent was not a valid legal basis given the imbalance of power between the data subject and the controller.<sup>68</sup>

In March 2023 **the Welsh Senedd** backed a call<sup>69</sup> for legislation over the use of biometric data in schools led by Sarah Murphy, member for Bridgend:

*"when it comes to this, it actually is really important that we do look at it through the lens of our values, our culture and our human rights—the children's human rights, and the power dynamics and the power exchange that is happening here on our watch, where our children, as we have heard, have no autonomy and no right to education free from surveillance. As the Manic Street Preachers sing, 'If you tolerate this, then your children will be next.'"*

By contrast, in July this year, when the ICO issued a reprimand to Chelmer Valley High School, in Chelmsford, Essex that broke the law when it introduced facial recognition technology (FRT)<sup>70</sup> it said:

*"We don't want this to deter other schools from embracing new technologies. But this must be done correctly with data protection at the forefront, championing trust, protecting children's privacy and safeguarding their rights."*

In both this case and in Scotland, **the ICO reprimands stopped at the school**. There were no fines, nothing was banned, and the regulator did not investigate the distributor as data processor, or likely controller role for its product improvement. **The company continues to enable unlawful introductions and offer cost-free 'upgrades' from fingerprint to facial recognition with no independent quality or standards oversight, in the same manner so that schools get it wrong, again, and again, and again.**<sup>71</sup>

<sup>66</sup> HEPI (2024) "more than 50% students have used genAI for help on assessments 5% likely using it to cheat" <https://www.hepi.ac.uk/2024/02/01/new-hepi-policy-note-finds-more-than-half-of-students-have-used-generative-ai-for-help-on-assessments-but-only-5-likely-to-be-using-ai-to-cheat/>

<sup>67</sup> Christakis, (2020). First Ever Decision of a French Court Applying GDPR to Facial Recognition <https://ai-regulation.com/first-decision-ever-of-a-french-court-applying-gdpr-to-facial-recognition/>

<sup>68</sup> BBC (2019) Sweden – Facial recognition: School ID checks lead to GDPR fine. <https://www.bbc.co.uk/news/technology-49489154>

<sup>69</sup> Wales: Senedd backs call for legislation over the use of biometric data in schools (2023) Deeside news. <https://www.deeside.com/senedd-backs-call-for-legislation-over-the-use-of-biometric-data-in-schools/>

<sup>70</sup> Essex school reprimanded after using facial recognition technology for canteen payments <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/07/essex-school-reprimanded-after-using-facial-recognition-technology-for-canteen-payments/>

<sup>71</sup> Summer 2024 IT professional forum discussion of new FRT and biometric technology rollouts <https://www.edugeek.net/forums/educational-software/238642-crb-cunnighams-cashless-catering-facial-recognition.html>

Our children are less protected than others **outside the EU AI Act that regulates the use of Artificial Intelligence in educational settings as high risk and banned some processing that we continue here in the UK**, such as tools that claim to do emotional detection and predictive scoring. Our children are unprotected as we now lie **outside the EU Charter of Fundamental Rights**, and in England, the Westminster government has **not adopted the UNCRC into domestic law**, despite best efforts in Scotland and Wales, so we have inconsistency in approaches and protections.

#### 4. Data Use and Access Bill conclusions

**The Bill proposals fail to take account of these issues.** Lupton and Williamson concluded in their work on the datafied child in 2017, that in regard to the datafication and dataveillance of children,

*“the embodied and subjective voices of children are displaced by the supposed impartial objectivity provided by the technological mouthpieces of data...data are positioned in ways that override the rights of children to speak for themselves.”*

*“There remains little evidence that specific instruments to safeguard children's rights in relation to dataveillance have been developed or implemented, and further attention needs to be paid to these issues.”<sup>72</sup>*

**The Council of Europe published Guidelines for Data Protection in Educational Settings in 2020<sup>73</sup>** but the UK government has not adopted these into practice or nor ensured that settings have a means to do so for the 10 million children currently in education today.<sup>74</sup>

In November 2023 Baroness Kidron led a **House of Lords short debate on Educational Technology<sup>75</sup>** and she summed up,

*“Education is an extremely precious contribution to child development and widely regarded as a public good. It must not be undermined by allowing an unregulated market to develop without regard for the learning, privacy and safety of children.”*

Since Defend Digital Me first proposed a Code of Practice for data processing in educational settings, the unlawful practice, massive-scale data breaches, leaks and hacks, have escalated unabated. The intrusive nature of the types of data processing and the level of risk of processing, involving ever more biometrics and even now neuro and emotional tech, just keeps growing.

Companies are not only calling the shots but have taken advantage of the non-consensual education environment where children have no choice, cannot say no, and cannot control how their lives are being steered and surveilled by thousands of strangers who are now in the classroom and go home with children when they take their app-laden school devices home, even into their bedrooms.

After 10 years spent researching data practices in the UK education sector, and in our work with the 46 member states of the Council of Europe and with other European civil society organisations, **Defend Digital Me is of the opinion that UK school children in state education are the least protected in domestic law and practice.** Our 2018 Data Protection Act extended the use of data from the GDPR but did not carry over the necessary safeguards. And our practice uses a far greater number and range of edTech companies and products in particular in the use of biometrics, than anywhere else.

The 2024 Bill not only sets the framing for more use and access, it has even removed the word ‘protection’ from the name of the Bill.

<sup>72</sup> **Williamson and Lupton (2017) The datafied child: The dataveillance of children and implications for their rights** <https://journals.sagepub.com/doi/abs/10.1177/1461444816686328>

<sup>73</sup> **Children's data protection in an education setting - Guidelines (2021) Council of Europe.** <https://edoc.coe.int/en/children-and-the-internet/9620-childrens-data-protection-in-an-education-setting-guidelines.html>

<sup>74</sup> **How many pupils are there in the UK?** Besa factsheet using DfE data <https://www.besa.org.uk/key-uk-education-statistics/>

<sup>75</sup> **House of Lords short debate on Educational Technology Vol. 834** <https://hansard.parliament.uk/lords/2023-11-23/debates/0588AF21-816D-4556-9D84-93D9A2385A07/EducationalTechnology>



**Children in UK classrooms are widely used as ‘guinea pigs’ in trials of commercial products without any ethics committee reviews or any oversight of trained and accredited researchers.** Products trials can be brought into classrooms by anyone, as long as the school says yes.

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.<sup>76</sup> But they fail to state that instead, if using public task, it is obligatory to offer a right to object and a balancing test.

**SafetyTech company staff where the ‘safeguarding in schools’ is run through a managed service, or some cloud based providers, are able to see children’s nudes and highly sensitive data sent to the company from children’s devices, Defend Digital Me had confirmed from three of the leading “safetyTech” firms in England** in January 2024 and there is no accountability at the Department for Education to put any regulations into practice or law to prevent misuse, where one team is responsible for technical standards and another for schools guidance.

The commercial digital market in England’s schools is vast and no body has oversight of this, or vetting of apps or the introduction of Internet connected objects (IoT)<sup>77</sup> in the classroom. **Teacher training lacks any standard content on child rights, data protection and privacy.**

**There are new plans underway for a national content store, taking children’s written work into a repository for AI companies to extract and build their own AI commercial products.**

In 2017, in the drafting of the UK Data Protection Act 2018, peers debated the introduction of a Code of Practice for educational settings in the name of the Earl of Clancarty. Nothing was done.

**Learners need protection now. They cannot wait for the DfE to come good on its so far empty promises to create change or to tell people what the Department itself does with pupil data.**

Saying tomorrow, and tomorrow and tomorrow, signifying nothing, is not good enough.

---

November 2024

\*Amended post-publication, to note that of the 32 Scottish Authorities, only half participated through to completion.

## **About Defend Digital Me**

Defend Digital Me 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.

### **Contact**

Jen Persson

jen@defenddigitalme.org

w: <http://defenddigitalme.org>

---

<sup>76</sup> **EdTech Innovation Testbed: FAQs for schools and colleges**

<https://www.nesta.org.uk/project/edtech-innovation-testbed/frequently-asked-questions/>

<sup>77</sup> **The Blakett Review (2014)** of IoT.