Data Use and Access Bill, House of Commons Committee Stage (2025) Background Briefing v1.7

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. http://defenddigitalme.org

Contact
Jen Persson

Summary recommendations

This Bill takes things away but does not build better. This comments only on the Bill as drafted. Explicit safeguards are still missing that the GDPR requires in several places but were left out of the UK 2018 drafting, or are being further reduced by this Bill. Defend Digital Me commissioned a Legal Opinion by Stephen Cragg KC of Doughty Street Chambers relating to the Data Protection and Digital Information Bill (2023) and many of the remarks remain applicable for this revised version of the Bill.

1.Recommendation one: Undo change that scraps human responsibility for computer decisions

Automated decision-making: Clause 80 in the DUA Bill (automated decision-making) does not address the necessary safeguards required in GDPR 23(1) for children (or anyone else) to be applied to Article 22 of the GDPR. As currently drafted, Clause 80 weakens protections for automated decisions (meaning that computers can have a significant effect on people's lives without the protection of another human's involvement). The safeguards are too weak to prevent unsafe practice in the world where more and more is automated and people feel like they need to take back control. This practical change in data protection law has dire human, economic, social and political consequences, e.g. Case studies that caused harm and this clause would risk normalising: AI claiming to identify student loans fraud, predictive algorithms used in children's social care.[1]

Change: Undo the connected Clause 80 changes in the Bill that remove these protections from current law. Leave the prohibition in place on solely automated decisions based on personal data.

2.Recommendation two: Undo changes that scrap risk assessment for vulnerable individuals

The Legitimate Interests new Condition (Part IV) Schedule 1, parts 6-8

A list of 'legitimate interests' has been elevated to a position where the fundamental rights of data subjects (including children as well as the elderly) can effectively be ignored as long as the data controller claims the persons were vulnerable, where the processing of personal data is concerned. The Secretary of State can add to this list without the need for primary legislation, bypassing Parliamentary scrutiny without **added protections for the personal data of individuals.**

The new condition removes the current protections of the balancing test or Right to Object and will expose vulnerable individuals to new risks where there is less transparency to the data subjects no oversight of what risks were determined to be fair to infringe upon rights and no remedy since the right to object / opt out of that processing is removed. The condition is also *open-ended* since there is *no obligation to assess vulnerability or to determine when the condition is no longer valid.* It is unclear what are the use cases where this should ever be applied other than to disregard protections in the current law today – what is the problem this change is trying to solve? It is likely any 'barriers to data access in today's law are a result of poor understanding, poor training, and poor practice and these do not require a change of law but changes in capability of staff working with 'vulnerable individuals'.

Recommended change: Remove the Legitimate Interests condition for Vulnerable Individuals
Compromise changes: require controllers to make an assessment of vulnerability, make it available to the data subjects and at minimum on an annual basis for any subsequent processing. Amend the new condition further to ensure it must cease to apply when the nature of the vulnerability for the individual, or the type of individual, is no longer present or has otherwise expired.

3.Recommendation three: Remove the changes that reduce information for data subjects

Change: Remove Clause 77 (Information to be provided for data subjects) and leave the current duty in place as it is. It does not need to be changed. It may not be enforced today, but this should not mean we change the law to make current unlawful practice lawful.

[1] Press, T.A. (2022) 'Oregon is dropping an artificial intelligence tool used in child welfare system', *NPR*, 2 June. https://www.npr.org/2022/06/02/1102661376/oregon-drops-artificial-intelligence-child-abuse-cases

Clause 77 will remove the current duty to provide information to data subjects when personal data is processed for a further, separate, purpose if it is for scientific research and (the controller decides) it would require 'disproportionate effort' to provide information. This lessens today's rights. This overrides the fundamental first principle of data protection law, domestic and international, fair processing, telling people in routine circumstances, what is done with information about them. This duty should instead ensure public trust in the State, limit unforeseen exploitation by commercial data processing and in effect ensure there are,"no surprises". This is the only way you get told of data rights associated with any of your data processing at scale, and to scrap not only being told, but therefore told about any of your data rights, is disastrous in the age of AI.

4. Recommendation four: Do not reduce Purpose limitation or permit Stretching of Consent

Change: Remove Clauses 68 and 71, purpose limitation and related clauses, and leave the current duty in place as it is unchanged. The same reasoning is how the personal confidential and even sensitive data from all state educated pupils aged under 48 has been given away as identifying data to third parties since 2012. This is not a model to copy.

Clause 68 and 71 will enable the "stretching" of consent to other purposes when personal data is processed for a further, separate, purpose if it is for scientific research and (the controller or the Secretary of State can decide) but without the hardwired safeguards of GDPR Article 89.

5. Recommendation five: Ensure the Bill does not Infringe on Privacy by Accident

Add a new Clause to adapt recital 57 of the GDPR on the face of the Bill: "*A controller shall not obtain or process additional information solely to identify a data subject who they cannot already, for the purpose of complying with any provision of the UK GDPR or this Act."*

This provision aligns with the principle of data minimisation under Article 5(1)(c) of the UK GDPR and aims to reduce unnecessary processing while respecting data subjects' rights. This Bill makes a number of provisions around identity and children, with implications for identification and continued retention of data about age, data which the controller or processor may not otherwise possess.

6. Recommendation six: New Clause to prevent excessive Biometric data retention in Schools

Add **a new Clause to prohibit Retention of Children's Biometric data** in Chapter 2 of the Protection of Freedoms Act 2012, Section 26.

Today consent is given generally by parents on behalf of the child, often during the school admissions process when a child is aged 10-11 often in a "home-school agreement" without destruction date. Many MPs might find their child's or even their own biometric data are still being processed by companies collected in educational settings, long after they leave school. Consent obtained for the processing of a child's biometric data should instead automatically expire when a child is deregistered from an educational setting. The relevant authority must receive written assurance of the destruction of a child's biometric information, from each of its processors or controllers by virtue of this section, no later than one calendar month after a child has been deregistered from the educational setting, and make the notice available to the child.

7. Recommendation seven: Clarify scope of commitment to a Code of Practice in Education

Clarify the commitment made to an ICO Code of Practice on processing personal data in education, coming from the Lords. Will the minister confirm a timeline for when the direction, committed to at the dispatch box on January 28, 2025[2]will be issued to the ICO and clarify that the scope of the Code of Practice will cover data protection across the education sector, including all data processing and not only edTech, and what the expected timeline for its delivery might be?

8. Recommendation eight: Keep the public interest element in Clause 67 added in the Lords

Government amendment to Clause 67 should not be made, as it undoes the safeguard Lords added.

[2] https://defenddigitalme.org/2025/01/29/dua-bill-amendments-and-commitments-made-in-report/

Background and case studies underpinning each proposed change

1. Automated decisions need more safeguards in place, but this Bill scraps them

The Bill takes away the safeguards in place in law today that require a human to have accountability and ensures that automated decisions cannot be 'fully' automated. This Bill only makes provision for safeguards where sensitive data is used (a particular designation in data protection law for example religion, ethnicity, biometrics, and union membership).

In Committee Stage of the Bill, Lord Clement-Jones said,[3]

> *"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.*"

A significant decision must never be taken based solely on automated processing. Computer-led decisions without meaningful human involvement have ruined lives in the Post-Office Horizon scandal, seen hundreds of students protesting on the streets, in the Netherlands the government was forced to resign after their attempts to use automated processes for fraud detection in welfare payment systems had disastrous societal consequences.[4]

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 profiling, and recommended it was forbidden for children and persons who cannot freely express their consent, especially, for example, adults with incapacity:

> *"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."* (p46)

In the UK profiling is rife across the public sector and growing in its applications (from Troubled Families 'tick box criteria to qualify' to profiling parents as welfare benefits' recipients 'risk factors' for fraud with severe knock-on implications for children where errors have long term harm and no route for immediate remedy.

A number of Higher Education students who reported estrangement from their parents when applying for student finance reportedly had their social media monitored by the Student Loans Company searching for proof that the students had made false claims and had contact with their parents. Several students had their loan payments stopped, and some reportedly dropped out of university, despite no findings of fraud against them.[5] Elsewhere, these are the kinds of monitoring increasingly done by computer scanning and without any humanity in individual cases.

In the 2020 summer examinations under COVID, almost 40% of students received grades lower than they had anticipated,[6] sparking public outcry and legal action. **Thousands of children were graded by algorithm, and we saw furious student protests at the DfE**.[7] 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 lack of accountability and remedy have not changed.

---

[3] Data Use and Access Bill Hansard (December 18, 2024) HOL
https://hansard.parliament.uk/Lords/2024-12-18/debates/A1CA5CDE-6F55-42E6-8153-31F3FFB302E4/Data(UseAndAccess)Bill(HL)
[4] The "SyRI" welfare fraud risk-scoring algorithm *Digital Freedom Fund*. (pronounced like "Siri")
https://digitalfreedomfund.org/the-syri-welfare-fraud-risk-scoring-algorithm/
[5] Adams, R. (2018) Student loans firm accused of "KGB tactics" for assessing eligibility. The Guardian.
https://www.theguardian.com/education/2018/oct/30/student-loans-firm-accused-of-kgb-tactics-for-assessing-eligibility
[6] 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/
[7] BBC (2020) A-levels and GCSEs: Boris Johnson blames 'mutant algorithm' for exam fiasco
https://www.bbc.co.uk/news/education-53923279

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**.[8]
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 biometric recognition technologies in schools including automated decisions**.[9]

Baroness Falkner said,[10]

> "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".

Case study: AI tools are sold without evidence of quality to 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 scrapped after it did not "realise the expected benefits**".[11] "There are widespread conditions of poor data quality and questionable data collection and recording practices and amplifying, historical patterns of systemic bias and discrimination.[12] 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 is scrambled to the point of uselessness in any case****."*[13]

Case study: These systems when used in *policing* have dire consequences for children and restrict their access to education and opportunity. Big Brother Watch covers these matters in more detail.[14]

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 clarificatio****n*." 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.

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 fact, profiling and solely automated systems fail everyone, not only children.

---

[8] 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/
[9] 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
[10] 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
[11] 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/
[12] 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
[13] 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/
[14] **BBW briefing (February 2025**) from page 16 https://bigbrotherwatch.org.uk/wp-content/uploads/2025/02/Big-Brother-Watchs-Briefing-on-the-Data-Use-and-Access-Bill-for-Second-Reading-HoC-2025.pdf

2. The legitimate interests special condition Schedule 4, Annex 1, parts 6-8

Lady Jones of Whitchurch, who until Christmas was the minister leading the Bill, raised concerns about the broad nature of the new LI objectives in 2024 in Opposition. She rightly said:

> "*There is no strong reason for needing that extra power, so, to push back a little on the Minister, why, specifically, is it felt necessary? If it were a public safety interest, or one of the other examples he gave, it seems to me that that would come under the existing list of public interests"* [Hansard, 25/3/24; col. GC 106.]

These clauses in the Bill as it stands, introduce a grave risk of disregarding protections for people's rights at exactly the time when they most need them, in time of vulnerability, and then extending that disregard in perpetuity because the condition is unlimited in time. If someone is in urgent need of support, the LI basis is **not** what is used in data protection law, but the lawful basis of "vital interests" is used instead. And in cases where there is an immediate need to act, there is no barrier to do so under current data protection law.

Bill Part 8(b) explains that this can be used with adults over 18 and relating to a particular individual and protection relating to ***a type*** of individual [our emphasis]. For example, "the elderly".

The current wording today in law on Legitimate Interests of Article 6(1)(f) sets out a balancing test which permits processing for any 'legitimate interest' purpose, ***provided that*** the processing:-

> …is necessary for those interests, ***except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject*** which require protection of personal data, ***in particular where the data subject is a child.***

This Bill ignores this completely and goes in the opposite direction to ignore these interests **in particular where the data subject is a child** (by being deemed by default vulnerable). In effect, this justifies that the processing of personal data meets the requirement of 'necessity' and therefore no longer needs the fundamental rights 'balancing' test. It also means likely this change will be used as a blanket group exemption for "a type" e.g. "for children" or "for the elderly" and without any assessment of whether there is in fact necessity in each and every case. This means other rights are then disregarded en masse, such as the right to object or opt out – a key failure for example if it is with AI or automated decision-making where LI is the common basis for data processing.

This Bill abandons this global standard and enables processing of personal data to be treated *for certain* as processing in a manner compatible with the original purpose and that do not require a risk assessment to meet today's standard[15] with safeguards in place that where the Secretary of State applies a restriction it must, *"respect the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society*".

Not only for the purposes of scientific research or historical research, (ii) for the purposes of archiving in the public interest, or (iii) for statistical purposes with Secretary of State powers which are generally but not always considered compatible, but by virtue of page 81 (3)(d) the processing meets a condition in Annex 2 (p.194).

Today those conditions are *not* set in stone in the GDPR or UK GDPR Article 6(4) but must be assessed to see if they are compatible [16] based on context and the people involved, and where it is determined upon *assessment of risks* through the balancing test that respect for the *essence of the fundamental rights and freedoms* of the people involved is **ensured**. This Bill scraps risk assessment.

[15] Article 23 https://www.legislation.gov.uk/eur/2016/679/article/23
[16] UKGDPR Article 6(4) https://www.legislation.gov.uk/eur/2016/679/article/6?

It is clear that these ‘clarifications’ in the Bill are intended to benefit data processors and controllers while providing no new protections for individual data subjects but there are no evidenced justifications.

This is so significant that it raises uncertainty whether data protection would be considered *adequate*, (whether the same level of data protection could be expected in the UK as in the EU or whether we have fallen below the expected standard which matters for allowing continued business and trade). On the similar draft proposals in the Bill’s prior incarnation, the Data Protection and Digital Information Bill (DPDI Bill) in 2023, **The European Commission (2.8.2023) raised the alarm**, saying,

> *“While a number of those amendments are aimed at clarifying the existing framework, some specific proposals would - if adopted - raise questions with respect to the level of protection. This is, for example, the case for [...] the proposal to give to the Secretary of State the power to recognise in the future certain interests of the data controller as a legal basis for processing (so-called ‘legitimate interests’) without any limitation and without the need for a balancing against the rights and interests of the individual. The Commission has repeatedly raised these concerns with the UK government and will continue to closely monitor how the Bill evolves in the parliamentary process.”*[17]

Case study using Legitimate Interests of Article 6(1)(f) and children today

Children are increasingly being labelled with the blanket term “vulnerable”. This means that without any assessment, data controllers can use the new powers to disregard rights. Today this basis is already used badly for deeply intrusive monitoring of children routinely at home and at school, through ‘safetyTech’ imposed by schools with no opt out offered of surveillance by companies.

SafetyTech company staff where the ‘safeguarding in schools’ technology 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 five of the leading “safetyTech” firms in England in 2025 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.[18]
Download an explainer of routine digital behavioural monitoring 24/7 from Defend Digital Me here.[19]

Cameras and voice recording always on in the classroom and are often justified for “safeguarding” purposes. 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**.[20] Parents of infants at a primary school have 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 despite the fact that these cameras record the children’s and visitors faces and voice, or health data. Recordings from 360 degrees are retained from multiple cameras with high spec microphones, and segments are sent to a company for processing offsite.

This kind of processing on the basis of “legitimate interests” is clearly an overreach of today’s law, but will be even harder to challenge if this condition is put on the face of the Bill and legitimised. There are no clear use cases that demonstrate its necessity, and in our view, the change will do harm.

---

[17] EN E-001790/2023, Answer given by Mr Reynders on behalf of the European Commission (2.8.2023) https://www.europarl.europa.eu/doceo/document/E-9-2023-001790-ASW_EN.pdf
[18] **DfE guidance: Meeting digital and technology standards in schools and colleges** https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges
[19] **Defend Digital Me 2025 explainer of School SafetyTech with recommendations for policy makers** https://defenddigitalme.org/wp-content/uploads/2025/01/DDM-digital-monitoring-action-slidedeck-2025.pdf
[20] **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/

3. Clause 67 Change Definition of Research (subclause 2 definition and safeguards)

Clause 67 -- the Minister Chris Bryant has proposed an amendment to the Bill in this Committee Stage that will remove a safeguard that the Lords put into the Bill.

Without the safeguard that the Lords put in, to require the use be "in the public interest" subclause 2 of clause 67 in the Bill will redefine 'scientific research' and 'scientific research purposes' in the Bill to mean **'any research that can *reasonably* be described a scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity**'.

This is an important change. It matters because defining something as research (that isn't already today) means that data users become *exempt* from some of the *other* key parts and protections for people in data protection law which are enjoyed by bona fide public interest researchers.

For example, today data protection offers some safeguard against the government simply handing over all our children's educational content and data to AI companies for development, as it plans to do later this year. If the Minister removes this safeguard, what else will protect us from endless commercial exploitation for product development or targeted marketing labelled scientific 'research'?

As Baroness Kidron explained on November 19th in the Lords this is <u>not</u> about 'tidying up recitals onto the face of the Bill'. View the Hansard contribution by Baroness Kidron (CB) on Tuesday 19 November 2024[21]

> "it will be insufficient to suggest that this is just tidying up the recitals of the GDPR. Recital 159 was deemed so inadequate that the European Data Protection Supervisor formally published the following opinion:[22]
>
> *"the special data protection regime for scientific research is understood to apply where … the research is carried out with the aim of growing society's collective knowledge and wellbeing, as opposed to serving primarily one or several private interests".*
>
> I have yet to see that the Government's proposal reflects this critical clarification, so I ask for some reassurance and query how the Government intend to account for the fact that, by putting a recital on the face of the Bill, it changes its status."

Furthermore: If use of personal data today that is not classified as research becomes classified as research in future, or if the definition is now possible for purely commercial research which includes technological development such as training AI products, it's not going to apply to *only* the data collected in future but to everything that's *already been ever collected* in the past to date. This means all of the public administrative data controlled by government. The strength of feeling about the reuse of creatives content shows this 'becoming AI training fodder by-default" is not what people want. Furthermore, the combination of this change with the change in clause 77 that removes the obligation to tell people, means the government could simply hand over all our personal data it holds, to commercial companies, and has made itself exempt from telling people.

---

[21] Hansard contribution by Baroness Kidron (CB) on Tuesday 19 November 2024 https://hansard.parliament.uk/Lords/2024-11-19/debates/6B196F71-312C-4957-AF14-98B66C5DBEE4/Data%28UseAndAccess%29Bill%28HL%29#contribution-1305C4D5-256F-4719-B6D7-F9A999EF44A6

[22] The European Data Protection Supervisor (EDPS) Opinion on Data Protection and Scientific Research (Page 12) https://www.edps.europa.eu/sites/default/files/publication/20-01-06_opinion_research_en.pdf

This would be in contravention of the fair processing obligation and as demonstrated in the well-known Bara case (ECHR Judgment in Case C-201/14)[23] that reiterates the obligation on public authorities to tell people whose data it is, what they do with our data, is against the spirit of DP law.

> *"The Court holds that EU law precludes the transfer and processing of personal data between two public administrative bodies without the persons concerned (data subjects) having been informed in advance."*

Case study: Commercial "research" reuse of public administrative data

The DfE already gives away pupil data for every child in state education, but no one has told parents and the 25 million people in the National Pupil Database (everyone aged under 48 in England today who was in state education, or took an exam like GCSE or A-levels even in private schools, including state educated MPs, their children or grandchildren for example). Commercial "research" reuses to date have included giving sensitive, and identifiable, pupil data to journalists, charities, think tanks and even a company that used it to make heat maps about school admissions for estate agents.

Parents of children in state education do not know about these commercial reuses, but recent public engagement work published by the DfE and DSIT[24] suggests they would want an opt-in to such reuse, to act as a control for them to be able to choose what is in the best interests of their child.

> "All participants expected to be involved in decisions made around the use of pupil's work **and data**, with parents and pupils having final say." (5.4)
>
> "Trust in tech companies was extremely limited and there was little to no support for them to be granted control over AI and pupil work **and data use**." (5.4) [our emphasis]

Furthermore, the volume of children's data to be controlled by the government is soon to be expanded for a whole new set of children and families who do not want their data commercially exploited by the state. In the 2024/5 Children's Wellbeing and Schools Bill, home educators' children's data will for the first time be sent to the Department for Education (DfE) under Clause 25, 436F. When combined with the Clause 67 of the Data Use and Access Bill, it would mean the DfE could now give away Home Educators' children's identifying data to companies for commercial research.

Home Educators (a) do not agree with HomeEd children's data being collected at child level (for which there is no need at national level) because these are not statistics or aggregated but at named child level and (b) do not want the change the government is trying to make to remove the protection of the children's commercial reuse.

Supplemental Briefing on the NPD:
https://defenddigitalme.org/wp-content/uploads/2024/05/NPD-Briefing-May-2024-v6.0.pdf

[23] Bara case (ECHR Judgment in Case C-201/14) reiterates the obligation on public authorities to tell people whose data it is, what they do with our data. https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150110en.pdf
[24] DfE and DSIT Public engagement (August 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

4. Clause 77 will remove the current duty to provide information to data subjects

This is a significant change. It will be used to override the fundamental first principle of global data protection laws, *fair processing*, telling people in routine circumstances, what is done with information about them. This duty should instead remain to ensure public trust in the State, limit unforeseen exploitation by commercial data processing, and there are"no surprises"[25].

Furthermore to repeat from example 6 above, the combination of this change with the change in clause 67 that changes teh definition of research, means the government could simply hand over all our personal data it holds, to commercial companies, and has made itself exempt from telling people. This would be in contravention of the fair processing obligation and as demonstrated in the well-known Bara case (ECHR Judgment in Case C-201/14)[26] that reiterates the obligation on public authorities to tell people whose data it is, what they do with our data, is against the spirit of DP law.

> *"The Court holds that EU law precludes the transfer and processing of personal data between two public administrative bodies without the persons concerned (data subjects) having been informed in advance."*

Where this duty is not met today, it must not be legitimised in the Bill and become an excuse to make what is unlawful lawful in future. For example, this duty is not met today, most notably, by the Department for Education as ICO found in its 2020 audit. If you do not get told of data processing, you are also uninformed of your rights associated with *any* of your data processing at scale, and to scrap this duty is disastrous in the age of AI.

This Bill could be used to continue to make that secrecy lawful. For the purposes of paragraph 5(b), whether providing the information "*would involve a disproportionate effort depends on, among other things, the number of data subjects, the age of the personal data*".

In situations where you are not told informed, data subjects will lose the ability to exercise all the other rights currently that are tied to the obligation to tell people about extensions of processing or to reconsent the data subjects, such as the rights to rectify, to restrict and to object to data processing.

The DfE also plans to enable re-use of data and content for AI development included in the planned changes to copyright law (consultation closing February 25th), **but will you be told, or asked for opt-out (it should be opt-in para 99-102) if this clause 77 passes?**

DfE/DSIT public engagement on the use of AI in education, published in August 2024, found, *"Trust in tech companies was extremely limited and there was little to no support for them to be granted control over AI and pupil work and data use. "*[27] *"...most parents described an "opt-in" model and expected to be given the chance to understand and agree to all potential uses of their child's data and work."* The last decade of public engagement about data from a variety of sources makes similar findings.

In Committee Stage of the Bill, Lord Jim Knight said, on December 18th 2024.

> *"My final cautionary tale, thanks to Defend Digital Me, is on the National Pupil Database, which was agreed in 2002 on the basis that children's data would be kept private, protected and used only for research purposes—all the things that we are hearing in the debates on this Bill. Ten years later, that was all changed and 2,500 data- sharing arrangements followed that use that data, including for universal credit fraud detection. When parents allow their*

[25] "No surprises" and its importance to public trust (2020) https://www.gov.uk/government/speeches/no-surprises
[26] Bara case (ECHR Judgment in Case C-201/14) reiterates the obligation on public authorities to tell people whose data it is, what they do with our data. https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150110en.pdf
[27] DfE/DSIT Research on public attitudes towards the use of AI in education (2024) GOV.UK. Available at: 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

> *children's data to be shared, they do not expect it to be used, down the line, to check universal credit entitlement. I do not think that was in the terms and conditions. There is an important issue here, and I hope that the Government are listening so that we make some progress."*

Five years after the DfE audit took place, **there is still no opt in for identifying sensitive personal data reuses or even any fair processing** (meaningfully informing the people whose data it is, what it is used for including to create heat maps for estate agents, for use by journalists, think tanks, charities, or for how long or why ("as required under Articles 12,13 and 14 of the GDPR"). [28]

Despite "fair processing" obligations set out in law–the duty to inform people how personal data is collected, used, and of our rights[29]—the majority of parents we polled through Survation in 2018, did not know the National Pupil Database exists. 69% of 1,004 parents replied that they had not been informed that the Department for Education might give away children's data to third parties.[30] The ICO noted in its audit that many parents and pupils are either entirely unaware of the school census and the inclusion of that information in the National Pupil Database "or are not aware of the nuances within the data collection, such as which data is compulsory and which is optional." (ICO, 2019)

In Committee Stage of the Bill, Lord Tim Clement Jones said,

> *"The findings back those of Defend Digital Me's Survation poll in 2018 and show that 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, the DWP, the Home Office and the police.*"[31]

If you or your children are state educated, this is your own personal confidential data at identifying level and you should be informed about its use, but this Clause will make not informing you, lawful. Millions of people do not know that their own or their child's identifying and sensitive (special category) personal data, that they trusted to a school only for the purposes of their nursery, primary, secondary or further education has been given to the Department for Education, and from there given away as identifying, individual level, sensitive data, for commercial reuses, think tanks, charities, journalists or academic researchers for over a decade, as well as widespread linkage with other data. 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.*"[32]

> ***"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."***

---

[28] Copy of the Executive summary of the ICO audit of the DfE 2020 with shocking failures on articles 12, 13 and 14 https://defenddigitalme.org/wp-content/uploads/2021/10/department-for-education-audit-executive-summary-marked-up-by-DDM-Jan-2021.pdf

[29] https://defenddigitalme.org/wp-content/uploads/2022/11/CBDS_RFC_1201_-_School_census_changes.pdf

[30] https://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables.pdf

[31] Data Use and Access Bill Hansard (December 18, 2024) HOL https://hansard.parliament.uk/Lords/2024-12-18/debates/A1CA5CDE-6F55-42E6-8153-31F3FFB302E4/Data(UseAndAccess)Bill(HL)

[32] 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
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/

Once pupils' data have left school systems and are sent to the DfE in the termly school census, the 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,[33] 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.*"[34]

Case Study: Five years after the audit took place, this Bill would make it more secret instead of fixing open issues:

- **There is still no fair processing** (telling the people whose data it is, what it is used for or where it goes for how long or why ("as required under Articles 12,13 and 14 of the GDPR");
- It is still not clear to schools as data controllers, what their role is in telling families what is collected under what law and what is optional, one of the key failings required by law highlighted in the summary of the audit that *was* published in October 2020;
- There is no apparent change in the "over reliance on public task" lack of identified supportive legislation, or the "limited understanding of the requirements of legitimate interest" necessary "to ensure the use of this lawful basis is appropriate and considers the requirements set out in Article 6(1)(f) of the GDPR" found (page 6/6);
- There is no right to object, balancing test and no opt out offered on the collection of, or the reuses of any sensitive and identifying pupil data from the NPD, at local or national levels;
- There is still no user-friendly Subject Access Request process, and not one suitable for children at all, or that 23 million people know about;
- And no way to know where your own data have gone or if it is still retained in any of the over 2,500 releases of identifying and sensitive data to third parties since 2012.

The data, at named pupil level, is highly sensitive and is constantly being expanded to include, for example, *Down Syndrome*. [35] 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.[36] 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[37] 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.[38]

In 2019 the DWP began requesting huge volumes of data from national pupil records[39] and 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.[40] Monthly handovers of pupil data continue to the Home Office which has sought matched details of nearly 7.2K individuals and the DfE has given the Home Office matched data from education records, for over one thousand eight hundred.[41]

---

[33] https://www.find-npd-data.education.gov.uk/categories

[34] **UIN 109113:"The DfE 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/

[35] **Young carer census label added 2022** https://defenddigitalme.org/wp-content/uploads/2022/11/CBDS_RFC_1201_-_School_census_changes.pdf

[36] **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

[37] **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

[38] **Gender identity field added to school information managements systems at DfE for local use (2023)** https://assets.publishing.service.gov.uk/media/642bf367fbe620000f17dbc7/CBDS_RFC_1233_-_Sex_and_Gender_Identity.pdf

[39] **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

[40] **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

[41] **External data shares between July 2024-July 2015** https://www.gov.uk/government/publications/dfe-external-data-shares

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".[42] The Reception Baseline Test began in 2021.[43] The DfE began collecting school attendance data daily on a named basis from every on-roll child in 2022[44] and the aggregated data from Local Authorities' registers of every child in Home Education in 2024. **Families are not told.**

In the last decade, none of the school census data expansions or new national primary tests were effectively communicated to parents with their rights. None ever offered a route to exercise a right to object or opt out, 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.

In Higher Education across the UK, equality data is collected and retained on a named basis in national databases via JISC[45] 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.**[46]

Higher education students are not informed of this and do not know they are on these lists.

You have the right to ask the DfE for a copy of your own, or your child's personal data from National Pupil Data and details of its source and where it has gone. Their process is online here https://www.gov.uk/government/publications/requesting-your-personal-information-from-dfe/requesting-your-personal-information-from-the-department-for-education.

Families must be offered an opt-in control over National Pupil Data reuse, This is possible to legislate for in this Bill and to create the mechanism for future AI content store management now.

Rather than legislating for the uses cases that remove the right to be informed, imagine if every use of data from a child could be accurate and kept up to date by parents and schools, rights exercised through the School Information Management System app on phones, the rights' controlled through existing systems with data fields and interoperability at the Department for Education to receive them.

---

5. Clauses 68 and 71 together enable the "stretching" of consent to other purposes

This is a significant combination of changes. Data protection standards for decades have required and rely on subsequent use after data is collected to be risk assessed to ensure it is 'not incompatible' with the original purpose for collection, going back to even the OECD 1980 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

What people believe they agreed to should not be undermined in future by being able to 'bend' consent to what researchers want but what the data subjects did not expressly agree to and the safeguards must be concrete not simply 'have regard to the existence of' as a tick box that exists somewhere undefined, but is not "in place".

---

[42] Multiplication Tables Check (MTC) begun (2019) Defend Digital Me
https://defenddigitalme.org/2019/05/10/the-multiplication-tables-check-mtc/
[43] Reception Baseline Test begun (2021)
https://defenddigitalme.org/2020/06/25/baseline-beaten-back-to-2021-time-for-change-in-the-accountability-system/
[44] 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/
[45] UIN HL4026 Equality monitoring data
https://questions-statements.parliament.uk/written-questions/detail/2024-04-23/HL4026/
[46] Equality monitoring 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/

Key to the change in the Bill Clause 71 is a proposed new Article 8A to the UK GDPR (introduced by clause 6(5) of the Bill) for the purposes of setting out the conditions under which further processing of personal data complies with the purpose limitation principle in Article 5(1)(b). The Bill (through this new Article) would add a new Annex to the UK GDPR listing situations in which processing is to be treated as compatible with the original purpose. In addition to the list in that Annex, the Bill also provides that a new purpose is compatible with the original one if the new purpose is to safeguard one of a number of public interests listed in Article 23(1)(c) to (j) to UK GDPR (largely to do with law enforcement and national security) and the processing is authorised by law.

However, 8A(3) (page 81) only suggests "In making the determination, a person must in (2)(e) "**take into account the existence of"** appropriate safeguards (for example, encryption or pseudonymisation)" but fails to adopt the accompanying hard-wired safeguard of Article 89 found in the GDPR, that **ensure** respect for data minimisation in processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,

> "**shall be** subject to appropriate safeguards, for the rights and freedoms of the data subject. Those safeguards **shall ensure** that technical and organisational measures **are in place** in particular in order **to ensure respect for the principle of data minimisation.** Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. **Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."**[47] [our emphasis]

Case study: failure to uphold rights when data use was expanded for 'research' purposes

This is the same reasoning behind how the National Pupil Database was moved in 2012 from being used only by the Department for Education to being made available to a wide range of third parties. In Scotland, parents are furious that data from the most sensitive and intrusive personal questions including some about detailed sexual behaviours and abuse, from a survey of pupils in state schools, are now being offered unexpectedly to third party researchers without tier permission or having been informed which unreasonably in their view, extends what they were told, that the data would be used by Local Authorities. This clause is a real risk to rights in combination with clauses 68 and 71.

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."[48]

In 2021 the Scottish government overruled the Scottish Children's Commissioner's request to pause the survey. Data protection law offered no protection and there is no route for recourse or remedy.

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.

[47] Article 89 of the GDPR Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes https://www.legislation.gov.uk/eur/2016/679/article/89
[48] 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/

This change is vital to be fit for future data uses. Today, genomic data is collected with poor consent practices from babies immediately after birth in the heel prick test. It is vital to uphold trust in this test as it is first used for the direct testing of several critical conditions that need to be identified at birth. However, it is then retained and parents are never asked again if they consent to a myriad of undefined 'research' purposes. Genetic data can never be anonymous.

> *"Residual newborn blood spots may also be used for research where the samples have been anonymised and the research project has ethical approval, as outlined in the Human Tissue Act and in MRC Guidance, 9 without individual informed consent."*[49]

Genomic data linked with pupil records in the future, means big risks and potential unintended consequences. The DfE and Government Office for Science have awarded a three-month £50,000 contract to look at the implications of future genomic technologies on the education sector, as reported by Schools Week in 2024.

The first foray by the Department for Education into predictive genetics wowed some people and a former well-known Spad at the DfE was a fan. In 2013 Professor Plomin described the role of genetics as "the elephant in the classroom" to the Education Select Committee.

Some researchers who have been pushing for genetic testing to become routine for the population at large are once again being given public platforms to promote their ideas. Others routinely encourage linkage of education data and much more to genomic data all without explicit, fully informed consent. Fundamentally, in what kind of society will children grow up? We are already the first country in the world to permit so called 'three parent children'. How far will we go down the path of 'fixing' prenatal genetic changes? How may this look in a society where 'some cornflakes get to the top' and genetic advantage is seen as a natural right over those without that ability? In a state where genetics could be considered as part of education planning? This is where consent above all matters in scientific and any other research, and consent should not be 'stretched' beyond what people agreed and expect.

---

6. New: Ensure the Bill does not have unintended consequences for new data

Add a new Clause to put recital 57 of the GDPR on the face of the Bill: "A controller shall not obtain or process additional information solely to identify a data subject who they cannot already, for the purpose of complying with any provision of the UK GDPR or this Act."

This amendment would ensure clarity around the principle set out in GDPR Recital 57, ensuring that controllers are not required to obtain additional identifying information in order to identify the data subject whom they cannot already, for the sole purpose of complying with any provision of this Regulation. This aligns with the principle of data minimisation, reducing unnecessary processing while respecting data subjects' rights. It is especially important since this Bill makes a number of provisions around identity and about children, with implications for identification and continued retention of data about age which the data controller or processor may not otherwise possess.

---

7. New: Better protect children's Biometric Data fit for the future

Add **a new Clause to prohibit Retention of Children's Biometric data** in Chapter 2 of the Protection of Freedoms Act 2012, Section 26.

Today consent is given generally by parents on behalf of the child, often during the school admissions process when a child is aged 10-11 often in a "home-school agreement" without destruction date.

[49] 2016 Consultation supporting document to change Codes of Practice on babies data retention in the heel prick test https://jenpersson.com/wp-content/uploads/2016/09/Code_of_Practice_for_the_Retention_and_Storage_of_Residual_Spots_2005.pdf

Many MPs might find their child's or even their own biometric data are still being processed by companies collected in educational settings, long after they leave school. Consent obtained for the processing of a child's biometric data should instead automatically expire when a child is deregistered from an educational setting. The relevant authority must receive written assurance of the destruction of a child's biometric information, from each of its processors or controllers by virtue of this section, no later than one calendar month after a child has been deregistered from the educational setting, and make the notice available to the child.

In 2021 schools in Scotland across North Ayrshire began using facial recognition[50] for pupils buying lunches in the school canteen[51] and the ICO had to step in as an emergency reaction.[52] 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.[53]

After Defend Digital Me national research in 2022[54], 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".[55]

Survation polled 1,004 parents of children aged 5-18 in state education in England on behalf of Defend Digital Me 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 were being used to infer mood and emotions. ViewSonic introduced a product in 2020 to UK classrooms using "AI algorithms" it claimed could monitor "*every student's facial expression for real-time tracking*" and identify one of five moods.[56] (Would be unlawful under the EU AI Act).

In March 2023 the Welsh Senedd backed a call [57]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.'"

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.[58]

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".

---

[50] Parliamentary briefing (2021) Facial Recognition in Schools https://lordslibrary.parliament.uk/facial-recognition-technology-in-schools/
[51] FT (2021) Facial Recognition Cameras arrive in UK School Canteens https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9
[52] 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
[53] 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
[54] The State of Biometrics report (2022) King, P. and Persson, J. https://defenddigitalme.org/research/state-biometrics-2022/
[55] Sample school notice on FSM and fingerprint systems https://buxtonschool.s3.amazonaws.com/uploads/document/Biometrics-Policy.pdf?t=1731623500
[56] 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
[57] 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/
[58] 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/

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.[59]

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)[60] 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.[61]

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.

---

8. Clarification on Code of Practice in Educational Settings from Committee Stage

In Committee stage, the Minister gave a verbal commitment to giving the ICO a direction to create a Code of Practice for data protection in educational settings. But it was vague, and there should be more detail given as to what this commitment is, so that all the debate prior to this in the Bill and the amendments laid and then not put to a vote, after the verbal agreement, are given a fair chance of being discussed again if necessary.

We have discussed an ICO Code of Practice with peers since Lord Clancarty proposed amendment 117 in 2017, when Labour Lord Stevenson said accompanying explanations of what was going on with the National Pupil Database, "gave him a chill". It was proposed and debated subsequently by Labour MPs in the Commons, Liam Byrne, Louise Haigh, Chris Elmore and Darren Jones proposed a "*Code on processing personal data in educatio*n", but it did not pass in New Clause 16 in 2018. A "*Code of practice by Information Commissioner's Office on data sharing in relation to post-16 education*" was debated by peers again in 2021 with support from Lord Storey, Baroness Garden and Baroness Sherlock, and Baroness Kidron, and broadly again in 2022, in 2023. In 2024 peers called for a Code in debate led by Lord Clement-Jones recalling the work of Data, Tech & Black Communities, and expanded on by Baroness Kidron and Lord Russell, and supported in much more detail, with comments from Lord Jim Knight too, on December 18th 2024. The government must now commit to a full and thorough Data Protection Code for of Practice educational settings.

---

[59] BBC (2019) Sweden – Facial recognition: School ID checks lead to GDPR fine. https://www.bbc.co.uk/news/technology-49489154
[60] 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/
[61] 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

In 2020 the Council of Europe members states approved *Guidance for Educational Settings*[62] *under Convention 108* (data protection regulation that is directly applicable to the UK as a member state and in some ways more relevant now to the UK than even the GDPR since it no longer directly applies to us outside the EU). The UK has yet to implement the Guidance into any form of domestic statutory guidance or law. An ICO Code of Practice offers an opportunity to do this well, but must not row back on what was considered important in debate, and narrow the scope.

It is necessary at all, due to 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 via interactions with companies and their affiliates in the digital world. There have been no "lessons learned" or changes made in England to the oversight or procurement processes for technology used by children via schools, despite the case involving **a** convicted paedophile and former teacher who was identified in 2010 running a major UK education website.[63]

A code should breathe life into the explicit recommendation[64] 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)*

---

9. Children's voice and the UNCRC obligations

The Council of Europe 2022-27 Strategy on the Rights of the Child,[65] and UNCRC General Comment General comment No. 25 (2021)[66] 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.*

Participation of young people themselves has not been invited in the Bill development and the views of young people[67] 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 t****he need for clear and comprehensive information about pupil work and data use*** *and any potential*

[62] CoE Committee of Convention 108 adopted Guidelines on Children's Data Protection in an Education Setting (2020) https://www.coe.int/en/web/data-protection/-/protect-children-s-personal-data-in-education-setting-
[63] Paedophile ran teaching website (2010) BBC http://news.bbc.co.uk/1/hi/8462650.stm
[64] 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
[65] 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%2BcAAx34gC78FwvnmZXGFUl9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t
[66] 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%2BcAAx34gC78FwvnmZXGFUl9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t
[67] 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)

risks relating to data security and privacy breaches." (5.4)[68]

The Bill fails to take account of these attitudes. Lupton and Williamson concluded in 2017, that,

> *"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."* [69]

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. We use a far greater number and range of edTech companies and products in particular in the use of biometrics, than anywhere else.

States have obligations towards children's rights. As the UNCRC General Comment No. 16[70] on State Obligations regarding the Impact of the Business Sector on Children's Rights, set out in 2013:

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

Whether there is incompatibility with devolved nations in particular where the UNCRC has been adopted into domestic law in Scotland and in Wales, may remain to be seen in further debate.[71]

[68] 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

[69] 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

[70] UNCRC GC no.16 (2013) https://resourcecentre.savethechildren.net/pdf/7140.pdf/p.3 1.1 Introduction and objectives.

[71] Westminster power grab an affront to devolution claim Welsh politicians Sun 9th Feb 2025. *Wrexham.com*. https://wrexham.com/news/westminster-power-grab-an-affront-to-devolution-claim-welsh-politicians-265142.html

10. Proposed Amendments for the Data Use and Access Bill

Amendment to Schedule 4: Annex 1 Risk assessment of Vulnerable Individuals

page 193, in Schedule 4, Annex 1, section 8 at the end after the definition of "vulnerable individual" insert the following new sub-paragraph—

> "(c) this condition is met only where the controller has made an assessment of vulnerability and makes it available to the data subjects prior to processing, at minimum on an annual basis for any subsequent processing.

Member's explanatory statement

Transparency and accountability responsibilities must not be removed from data controllers when processing personal data for the purposes of safeguarding vulnerable individuals based on an undefined characteristic that may change over time, and may not apply forever. The data subjects may not be aware that they have been categorised as vulnerable and therefore data is being processed on the basis of legitimate interests without their knowledge, this will prevent them exercising any of their other data subject rights. A balancing test based on the data subject's case would be required under the law today. Instead, this change will be used as a blanket exemption e.g. "for children" or "for the elderly". Note this is separate from the 'vital interests' lawful basis.

Key areas for probing the intent include:

The draft Data Use and Access Bill – rewriting UK data protection law – removes safeguards from today's law, in particular the processing of vulnerable individuals for the purposes of undefined safeguarding aims. Stephen Cragg KC highlighted in his Opinion[72] on the prior version of the Bill, the DPDI Bill, some of these key areas of concern, including that the legitimate interests for the purposes of 'safeguarding' condition are drawn too widely and require safeguards throughout the life cycle of the data not only about removing conditions at the time of data collection. This amendment seeks to explore whether the government intends to remove transparency and accountability obligations from data controllers when processing personal data for the purposes of safeguarding vulnerable individuals based on an undefined characteristic that may change, and that may apply or not apply to any given individual at any point in time. If there is no assessment of vulnerability prior to processing, how can the condition ever be lawfully applied where it *only* applies to vulnerable individuals, and will they be kept in the dark about the data processing, which means they cannot exercise any other rights? The amendment raises questions about the practical implementation of safeguarding measures, including:

1. How data controllers determine vulnerability,
2. The mechanisms for ensuring that data subjects are informed and have visibility into assessments of their categorisation as vulnerable, affecting their data rights,
3. The balance between transparency, professional confidentiality, and the rights of data subjects and that the balancing test currently required will no longer be mandated.

The government should clarify whether it intends to remove safeguards and the ability to exercise all of the data subject's other rights forever from vulnerable individuals or maintain compliance with other data protection principles, or whether the exclusion is designed (as it is drawn) to last forever.

[72] Stephen Cragg KC Opinion on this Bill's previous version, the Data Protection and Information Bill (Nov 2023) https://defenddigitalme.org/wp-content/uploads/2023/11/KC-opinion-DPDI-Bill-27112023-Stephen-Cragg.pdf

Amendment to Schedule 4: Attribution of Vulnerability to Individuals

page 193, in Schedule 4, Annex 1, section 8 at the end after For the purposes of paragraph 7—, insert the following new sub-paragraph—

> "(d). The condition ceases to apply when the nature of the vulnerability for the individual, or the type of individual, is no longer present or has otherwise expired.

Member's explanatory statement

Clarification is required on the safeguards and processes for ensuring that processing activities tied to an undefined and changeable characteristic of 'vulnerability' do not persist unnecessarily or disproportionately.

Key areas for probing the intent of the Bill include:

This amendment seeks to clarify whether and how the conditions for processing personal data based on the vulnerability of an individual should expire when the individual's circumstances change. It raises the following questions for consideration

1. Time-Limited Processing: Should the processing of personal data for vulnerable individuals automatically continue when the vulnerability no longer exists? How and when is that to be assessed by data controllers and processors?
2. Assessment and Review: What mechanisms are in place to ensure that data controllers regularly assess whether the justification for processing based on vulnerability remains valid?
3. Impact on Data Subjects: Since data subjects who are vulnerable are also more susceptible to data exploitation and otherwise have a lack of protection or agency, can the government justify in what circumstances such a persistent condition would apply that would be proportionate to necessitate the removal of the data subject's rights to a balancing test and being offered an opt-out?
4. Practical Implementation: Are data controllers equipped to identify and act on changes in an individual's vulnerability in a timely and accurate manner and how will this not simply lead to lazy application of this weakening of the protections that should accompany legitimate interests and are (rightly) already necessary for processing under the basis of Vital Interests?
5. The reason this is important is that this is a key element of data protection law: "conditions" create certain permission or exemptions from other aspects of data protection law that protect people from their personal confidential data in ways they do not expect or would be compatible with their other rights, like human agency and dignity. If another adult has decided arbitrarily to remove someone's rights, there should be justification that can be if not challenged, at the time, at least scrutinised and challenged when the condition no longer applies. The drafting of the Bill as it is makes no distinction or limitation on this characteristic so a company could decide that it will simply use everyone's personal confidential data as adults that the company collected from those people as a child and retain the exemptions from the law to need to do a risk assessment or "balancing test" as it is called, forever. Whereas in data protection law, without the new condition the Bill creates, you would need to have greater respect for the data over time and a duty towards the people it is from.

Proposed New Clause: Information to Be Provided to Data Subjects

Page 92, in clause 77, at the end, insert the following new sub-paragraph—

(c) at the end insert—

"Exemptions from Data Protection law Article 13, Information and access to personal data; and Article 14, Information to be provided where personal data have not been obtained from the data subject; shall not apply where the data subject is a child at the time of data collection or at the time of any subsequent data processing.

Member's explanatory statement

The exemption regarding the obligation to provide information about further processing should not apply to children, since these purposes will be broadened if the definition of research is explicitly expanded as per clause 67 of the draft Bill, "whether carried out as a commercial or non-commercial activity". Article 12(1) of the GDPR necessitates informed processing to form part of the most fundamental adequate protection, in particular where data is collected from or about children that may have lifelong effects, and in the spirit and letter of GDPR recitals relevant for children (38) Special Protection of Children's Personal Data (58) The Principle of Transparency (59) Procedures for the Exercise of the Rights of the Data Subjects (60) Information Obligation (73) Restrictions of Rights and Principles. Commercial reuses of personal data necessitates stricter safeguards and transparency in such contexts since the long 'daisy chain' of multiple processors' reuse will otherwise become entirely unaccountable to the data subject, to a child, or as future adults. Informed processing is fundamental to public trust in data processing, and fundamental to data protection law.

Proposed New Clause: Prohibition on the Processing of Additional Identifying Data

Page 84, After Clause 72 (data protection principles) , insert the following new Clause—

*"***Prohibition on the Processing of Additional Identifying Data**

(1) A controller shall not obtain or process additional information solely to identify a data subject who they cannot already, for the purpose of complying with any provision of the UK GDPR or this Act.

Member's explanatory statement

This provision aligns with the principle of data minimisation under Article 5(1)(c) of the UK GDPR and aims to reduce unnecessary processing while respecting data subjects' rights.

This amendment ensures clarity around the principle set out in GDPR Recital 57, ensuring that controllers are not required to obtain additional identifying information in order to identify the data subject whom they cannot already, for the sole purpose of complying with any provision of this Regulation. This aligns with the principle of data minimisation, reducing unnecessary processing while respecting data subjects' rights. This is especially important since this Bill makes a number of provisions around identity and about children, with implications for identification and continued retention of data about age which the data controller or processor may not otherwise possess.

Proposed New Clause: Prohibition on Retention of Children's Biometric data

Page 100. After Clause 81, insert the following new Clause—

*"***Prohibition on the Retention of Children's Biometric data in educational settings**

In Chapter 2 of the Protection of Freedoms Act 2012, Section 26, At the end insert —

(8) Consent obtained for the processing of a child's biometric data shall expire when a child is deregistered from an educational setting. The school Data Protection Officer must receive written assurance of the destruction of a child's biometric information, from each of its processors or controllers by virtue of this section, no later than one calendar month after a child has been deregistered from the educational setting, and make the notice available to the child.

Member's explanatory statement

This provision aligns with the principle of data minimisation under Article 5(1)(c) of the UK GDPR and aims to reduce unnecessary processing of highly sensitive data after a child leaves an educational setting. Today consent is given generally by parents on behalf of the child, often during the school admissions process when a child is aged 10-11 often in a "home-school agreement" without destruction date. Therefore, permission is granted, but companies are under no explicit obligation to cease processing until consent is withdrawn, although the necessity for its retention may have expired. Many MPs might find their child's or even their own biometric data are still being processed by companies collected in educational settings, long after they leave school.